République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique
UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

de MASTER ACADEMIQUE

Spécialité : Réseau et télécommunication

Filière : Génie électrique

Présenté par

Belhadj Belaid
Hamadouche Yacine

Mémoire encadré par ATTAF.Y et codirigé par KIBOUH.M

Thème

Etude et sécurisation d'une infrastructure DMZ avec ASA CISCO5510

Laboratoire et/ou entreprise où le travail a été réalisé : 2intparteners

Promotion: 2015

Remerciements

Nous remercions tout d'abord, Allah qui nous donné la force et le courage pour terminer nos études et élaborer ce modeste travail.

Nous tenons à exprimer nos plus sincères remerciements notre promoteur Mr. Attaf, qui nous a aider au long du travail.

Un grand merci à notre Co-promoteur Mr. Kibouh (2int) pour ses encouragements et ses orientations qui nous ont beaucoup aidés au cours de notre projet.

Nous sommes aussi reconnaissants à Mr. Zarouki qui nous a aussi soutenus et un grand merci à Mr. Larbi l'étudiant 2éme année master informatique pour ses informations qui nous a beaucoup servis.

Nous tenons à remercier également nos amis (es) et nos familles pour leurs aides considérables.

Sommaire

Sommaire

Sommaire

Chapitre II : Etude de l'existant

Sommaire

Sommaire

Chapitre III : Réalisation de l'application

Sommaire

Sommaire

Sommaire

Chapitre II : Etude de l'existant

Sommaire

Sommaire

Chapitre III : Réalisation de l'application

LISTE DES FIGURES 2014/2015

Glossaire 2014/2015

AIM Adaptive Identification and Mitigation

ACL Access Control Entry

AIP SSM Advanced Inspection and Prevention Security Services Module

ARP Adress resolution protocol

ASA Adaptive Security Appliance

ASDM Adaptive Security Device Manager

CA Certificate Authority

CSC SSM Content Security and Control SecurityServices Module

CIFS (Common Internet File System)

DDoS Distributed Denial-of-Service a

DMZ Demilitarized zone

DNS Domain Name System

FTP File Transfer Protocol

GNS3 Graphical Network Simulator

HTTPS Hypertext TransferProtocol secure

IDA Identity and Access

ICMP Internet Control Message Protocol

IDS Intrusion Detection Services

IIS Internet Information Services

IOS Inter-network Operating System

IP Internet Protocol

IPsec Internet Protocol Security

IPS Intrusion Prevention Services

LAN Local Area Network

MAC Media Access Control

MIB Management information base

MAN Métropolitain Area Network

Glossaire 2014/2015

NAT Network Address Translation

NFS Network File System

NCP Netware Core Protocol

OSI Open Systems Interconnection

PAT Port Address Translation

QOS Quality of Service

RADIUS Remote Authentication Dial In User Service

RAID Rendundant Array of Independent Disks

RPV Réseau privé virtuel

RPF Reverse Path Forwarding

SMB Server Message Block

SSH Secure Shell

SSL Secure Socket Layer

SNMP Simple Network Management Protocol

SMTP Simple Mail Transfer Protocol

SQL Structured Query Language

TCP Transfer Control Protocol

TFTP Trivial file Transfer Protocol ou protocole simplifié de fichiers

Telnet TélécommunicationsNetwork

USB Universal Serial Bus

VPN Virtual Private Network

VLAN Virtual Local Area Network

WAN Wide Area Network

Introduction générale

Un réseau informatique est un maillage de micro–ordinateurs interconnectés dans le but d'assurer le transfert de fichier, le partage des ressources (imprimantes et données),

L'exploitation de la messagerie où l'exécution de la maintenance de programmes à distance.

Quel que soit le type de système informatique utilisé au sein d'une entreprise, son interconnexion pour constituer un réseau est aujourd'hui indispensable. Les objectifs d'un réseau sont multiples, comme le partage des ressources informatiques entre les différents partenaires de l'entreprise (salariés, dirigeants, fournisseurs, etc..) et la transmission plus rapide des informations.

Aujourd'hui les entreprises utilisent de plus en plus d'informations, ce qui nécessite une meilleure organisation et de conditions de stockage optimales. L'outil informatique joue un rôle primordial sur ce plan. Pour faciliter la transmission de ces données informatisées, les entreprises s'organisent autour d'un réseau.

Le développement de l'utilisation d'internet, de plus en plus les entreprises ouvrent leur système d'information à des utilisateurs externes (partenaires, fournisseurs, membre de l'administration) au réseau local, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maitriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines vu l'expansion et l'importance grandissante des réseaux informatiques lesquels ces derniers ont engendré le problème de sécurité des systèmes d'information. Dans la plupart d'organisations informatisées, partager les données directement entre machines est leur souci majeur. Il s'avère indispensable de renforcer les mesures de sécurités dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Afin d'assurer le bon fonctionnement global de l'entreprise, on utilise une technique de la décomposition du réseau en zone de sécurités séparées est l'une des solutions les plus fiables que l'entreprise peut adapter pour protéger ses ressources matériels et logicielles.

Vu ses caractéristiques, est un moyen de lutter contre la violation potentielle du système de sécurité et les attaques contre la confidentialité .La bonne gestion de cette zone permet de minimiser les attaques venant du réseau externe, en autorisant les services dont l'entreprise a besoin. Cette décomposition appelée (DMZ) nécessite la mise en place d'un firewall pour pouvoir l'administrer.

L'ASA 5500 série est l'une des solutions proposée par Cisco. Elle met à la disposition une gamme complète de service personnalisé, à travers ses diverses éditions conçues spécifiquement pour le pare-feu. Ces différentes éditions offrent une protection de qualité supérieure en apportant à chaque installation les services dont elle a besoin de savoir les préventions des intrusions, la protection des contenus et les VPN…. etc.

L'objectif de ce projet est la mise en œuvre d'une infrastructure sécurisée par DMZ à l'aide de l'ASA Cisco 5510 en créant une stratégie de filtrage pour gérer le trafic entre les réseaux de l'entreprise et le réseau externe (internet).

Notre mémoire est réparti en trois chapitres, le premier chapitre présente des généralités sur les réseaux informatiques et les types de menaces, méthodes de protections…etc.

Dans le deuxième chapitre, nous exposerons un réseau dépourvu d'une DMZ, les critères du réseau existant ainsi une solution proposée…etc.

Le troisième chapitre sera consacré à la mise en place d'une infrastructure DMZ à l'aide de l'ASA. Enfin nous terminons par une conclusion générale.

I.1.Préambule

Les attaques informatiques ne cessent d'être dirigées contre les entreprises, En effet les réseaux dominent le monde informatique, les grandes entreprises ne peuvent plus survivre sans que leurs machines soient connectées à un réseau étendu (WAN ou Internet).

La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines de ce dernier fonctionnent d'une façon optimale. En conséquence, la mise en œuvre de la sécurité est indispensable au sein d'un réseau afin de le protéger de tout sort d'intrusion malveillante.

Dans ce chapitre nous avons présenté les différents aspects liés à la sécurité, les types d'attaques et leurs mécanismes de détection et la protection des réseaux informatiques

I.2.Définition d'un réseau informatique

Réseau (informatique) : ensemble d'ordinateurs et de terminaux interconnectés pour échanger des informations numériques.

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

- Réseau (Network) : Ensemble des ordinateurs et périphériques connectés les uns aux autres. Remarque : deux ordinateurs connectés constituent déjà un réseau).
- Mise en réseau (Networking) : Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources.

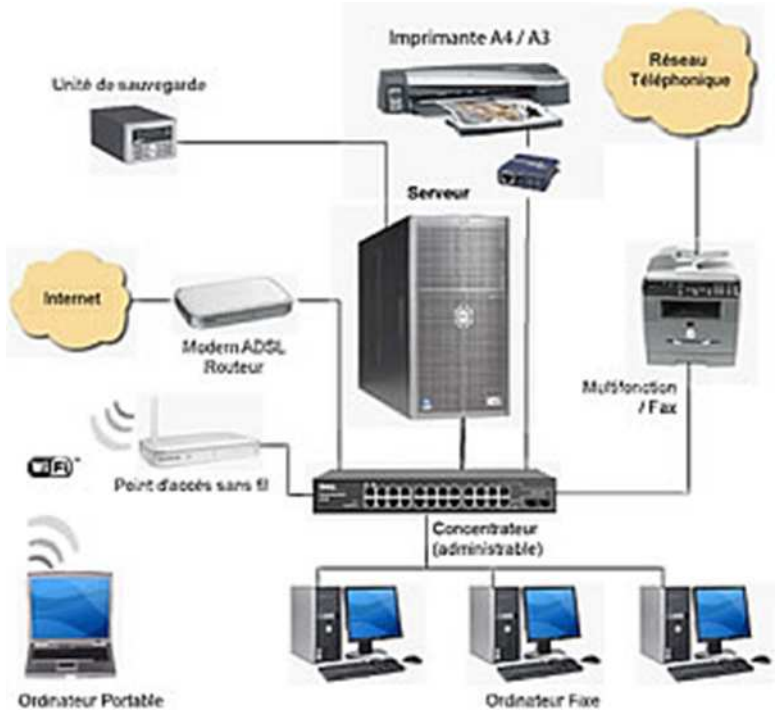


Figure I.1:réseau informatique

I.3.Architecture des réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories : réseaux poste à poste et réseaux à serveur dédie (client /serveur).

I.4.Classification des réseaux informatiques

On peut classer les réseaux selon plusieurs critères, par exemple la distance entre entités, communications, la topologie et le type d'accès.

- **Classification selon la taille**
  - Les réseaux locaux LAN (local area network).
  - Les réseaux MAN (métropolitain area network).
  - Les réseaux étendus WAN (wide area network).

- **Classification selon la Topologie**

- **Topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

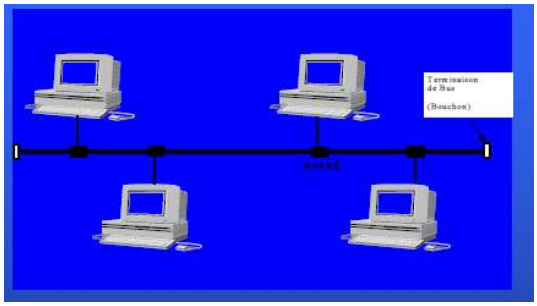


Figure I.2:Topologie en bus

Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

- **Topologie en anneau**

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole" successivement.

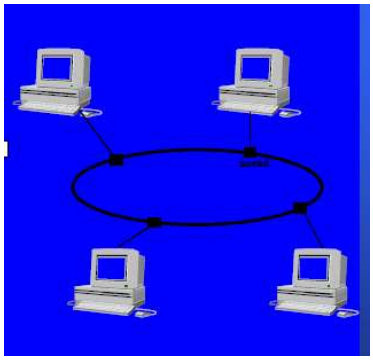


Figure I.3:Topologie en anneau

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole.

Les deux principales topologies logiques utilisant cette topologie physique sont TOKEN RING (anneau à jeton) et FDDI

- **Topologie en étoile**

  Chaque machine est reliée directement à un serveur et les données transitent à travers le nœud central.

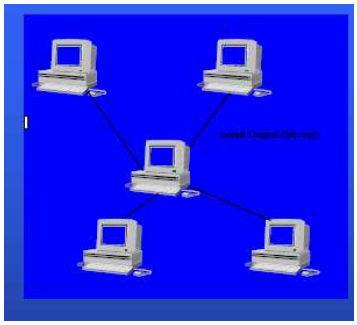


Figure I.4:Topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.

En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

❖ **Selon le mode de connexion**

- Mode avec connexion
- Mode sans connexion

❖ **Selon la méthode d'accès**

- Méthode d'accès CSMA/CD
- Méthode d'accès par Token ring
- Méthode d'accès par Standard FDDI

I.5.Interconnexion

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelles, Routeurs, Ponts …) qui assurent le transfert des données.

a. Les ponts

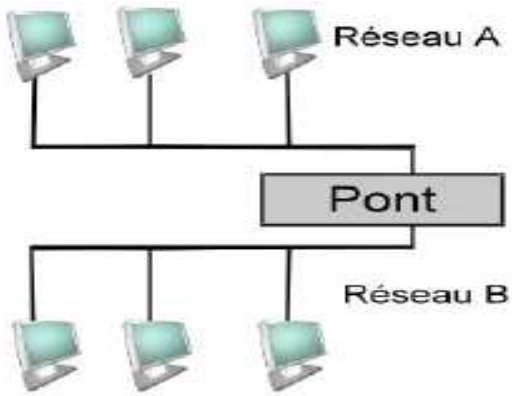


Figure I.5:les ponts

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont.

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel côté du réseau se trouve l'émetteur.

Ainsi le pont est capable de savoir si émetteur et destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau

b. Les Passerelles

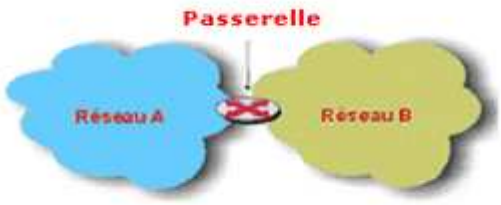


Figure I. 6:Les passerelles

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun des réseaux. Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données.

c. Les Routeur

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts). Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en termes de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation.

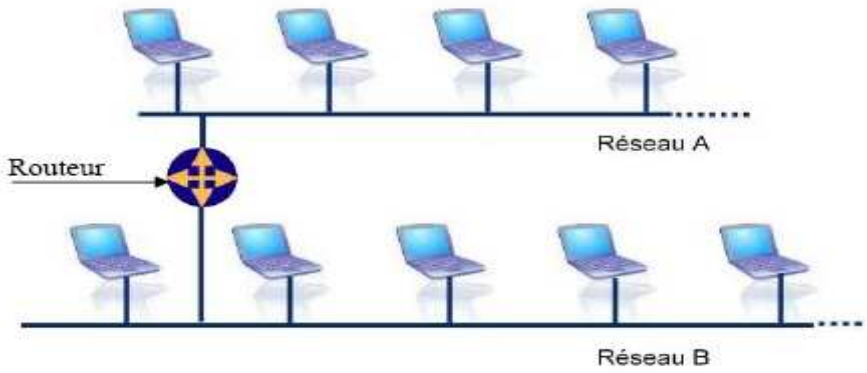


Figure I.7: les routeurs

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quel que soit l'architecture.

d. Les Hubs (concentrateurs)

Le Hub est également appelé concentrateur ou répétiteur. C'est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de

transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire).

e. Switch

Egalement appelé Commutateur, Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le Switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le Switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de données inutiles sur le réseau.

I.6.Les protocoles réseaux

I.6.1.Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers(FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP).

Sur Internet par exemple les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles reliés entre eux. Cette suite de protocole s'appelle TCP/IP.

I.6.2.Les différents protocoles réseaux

I.6.2.1.Protocole DNS

Le DNS (Domain Name System) est un système essentiel au fonctionnement d'Internet. C'est entre autres, le service qui permet d'établir la correspondance entre le nom de domaine et son adresse IP. L'échelle gigantesque à laquelle est déployé ce service rend le système capital pour le monde actuel, que ce soit pour des raisons financières, économiques ou politiques.

I.6.2.2.Protocole TCP

Est un protocole fiable ce Protocole sécurisé d'échange de données : créé dans le but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs autonomes et raccordés à un réseau (protocole orienté connexion).

I.6.2.3.Protocole IP

C’est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, Mais le rôle le plus important de ce protocole est d’acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les note sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255.

Par exemple, 194.153.205.26 est une adresse IP Ont peux distinguer deux parties dans une adresse IP:

- les nombres de gauche désignent le réseau (on l'appelle net ID)
- Les nombres de droite désignent les ordinateurs de ce réseau (on l'appelle host ID)

I.6.2.4.Protocole ICMP (Internet Contrôle Protocol)

C’est un protocole qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IP ne gère que le transport des paquets et ne permet pas l envois de messages d’erreurs, c’est grâce à ce protocole qu’une machine émettrice peut savoir qu’il y a eu un incident de réseau.

I.6.2.5.LE protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP aux équipements branchés au réseau. Lorsqu'un client essaie de se brancher au réseau, une demande de paramètres de configuration est envoyée au serveur DHCP. Une fois que le serveur a reçu le message, le serveur DHCP envoie une réponse au client, qui comprend les informations de configuration, puis enregistre en mémoire les adresses qui ont été attribuées. DHCP utilise le protocole BOOTP pour communiquer avec les clients.

Les clients doivent renouveler leur adresse IP à 50 % de la période d'utilisation, puis de nouveau à 87,5 %, en envoyant un message DHCPREQUEST. Les hôtes clients conservent leur adresse IP jusqu'à l'expiration de leur période d'utilisation, ou lorsqu'ils envoient une commande DHCPRELEASE. IPCONFIG et WINIPCFG sont des utilitaires exécutés à partir de la ligne de commande et qui permettent de vérifier les informations de l'adresse IP qui a été attribuée à l'hôte client.

I.6.2.6.Le protocole ARP

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse. Chaque machine connectée au réseau possède un numéro d'identification sur 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte réseau en usine.

Toutefois, la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme. On parle alors de l'adresse IP.

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête (contenant l'adresse de la machine demandée) sur le réseau. Chaque machine du réseau compare par la suite l'adresse logique reçue, avec la sienne.

Si l'une des machines s'identifie à cette adresse, elle répondra alors à ARP par une requête contenant son adresse physique, qui va stocker la couple d'adresses dans la table de correspondance et la communication va alors pouvoir serveur de messagerie électronique. Cette opération nécessite une connexion à un réseau TCP/IP.LE port utilise est le 110.

I.6.2.7.Protocole FTP (File Transfert Protocol)

Permet de transférer des fichiers d'une machine à une autre. L'utilisateur de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe .donc si l'utilisateur n'est pas reconnu la connexion ne sera pas établie.

I.6.2.8.Protocole SMTP (simple mail Transfer Protocol)

Est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messageries électronique. Il est assez facile de tester un serveur SMTP en utilisant le port 25.

I.6.2.9.HTTP (Hyper Text Transfer Protocol)

Est le protocole de communication du web permettant d'échangé des documents hyper textes contenants des données sous la forme de texte, d'images fixes ou animées et de sons. Tout client web communique avec le port 80 d'un serveur http.

I.6.2.10.Protocole Telnet

Le protocole Telnet est un protocole standard d'internet permet de relier les interfaces de terminaux et d'application à travers internet. Il s'appuie sur une connexion TCP sur le port 23 pour envoyer des données.

I.6.2.11.SNMP (Simple network Management Protocol)

Est un protocole communication qui permet aux administrateurs réseau de gérer les équipements de réseau, de superviser et de diagnostic des problèmes réseaux et matériels à distance.

I.6.2.12.TFTP (Trivial file Transfer Protocol ou protocole simplifié de fichiers)

Est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP.TFTP reste très pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare –feu, etc.) ou pour démarrer un pc à partir d'une carte réseau.

Pour assurer le bon fonctionnement du réseau et faire face aux menaces éventuelles qui peuvent le mettre hors service il est nécessaire de la sécurisé. Pour cela nous allons

présenter des notions sur la sécurité des réseaux informatiques dans le but de se familiariser avec les différentes menaces.

I.6.2.13.Le protocole 802.1xP

Le protocole 802.1x est une solution standard de sécurisation de réseaux mise au point par l'IEEE en 2001. 802.1x permet d'authentifier un utilisateur souhaitant accéder à un réseau (câblé ou Wifi) grâce à un serveur central d'authentification.

L'autre nom de 802.1x est "Port-based Network Access Control" ou "User Based Access Control". 802.1x permet de sécuriser l'accès à la couche 2 (liaison de donnée) du réseau.

Ainsi, tout utilisateur, qu'il soit interne ou non à l'entreprise, est dans l'obligation de s'authentifier avant de pouvoir faire quoi que soit sur le réseau. Certains équipements de réseau compatibles 802.1x peuvent réserver un traitement particulier aux utilisateurs non authentifiés, comme le placement dans un VLAN "guest", une sorte de quarantaine sans danger pour le reste du réseau.

802.1x a recours au protocole EAP (Extensible Authentification Protocol) qui constitue un support universel permettant le transport de différentes méthodes d'authentification qu'on retrouve dans les réseaux câblés ou sans-fil.

802.1x nécessite donc la présence d'un serveur d'authentification qui peut être un serveur RADIUS. un serveur Microsoft, Cisco (...) ou un produit libre comme (FreeRADIUS) ou encore un serveur TACACS dans le monde fermé des équipements Cisco.

Un port d'un commutateur réglé en mode 802.1x peut se trouver dans deux états distincts :

- État "contrôlé" si l'authentification auprès du serveur RADIUS a réussi.
- État "non contrôlé" si l'authentification a échoué.

La réussite ou l'échec de l'authentification va donc ouvrir ou fermer le port à toute communication. Un port ouvert va, par exemple, permettre au client final d'obtenir une adresse IP auprès d'un serveur DHCP.

Dans des implémentations plus cloisonnées, le serveur RADIUS indiquera par exemple au client RADIUS dans quel VLAN placer le client final.

I.11.Définition de la sécurité

Les réseaux sont des systèmes de stockage, de traitement et de circulation des données. Ils sont Constitués de composants de transmission (câbles, connexions radio, satellites, routeurs, Passerelles, commutateurs, etc.), et de services de soutien (système de noms de domaine incluant.

Le serveur de base, service d'identification de l'appelant, services d'authentification etc.). Il

Existent nombre surprenant d'applications liées aux réseaux (système de distribution d'e-mails, logiciel de navigation, etc.) et d'équipements terminaux (téléphones, ordinateurs hôtes, PC, téléphones mobiles, organisateurs personnels, appareils domestiques, machines industrielles, etc.).

Les exigences génériques de sécurité des réseaux et de l'information présentent les caractéristiques interdépendantes suivantes:

- **Disponibilité** – Signifie que les données sont accessibles et les services opérationnels, même en cas d'événements perturbants tels que des pannes de courant, des catastrophes naturelles, des accidents ou des attaques. Cette caractéristique est particulièrement importante lorsqu'une une défaillance du réseau de communication peut provoquer des pannes dans d'autres réseaux critiques tels que les transports aériens ou la fourniture d'électricité.
- **Authentification** – Confirmation de l'identité supposée d'entités ou d'utilisateurs. Des méthodes d'authentification appropriées sont nécessaires pour de nombreux services et applications, comme la conclusion d'un contrat en ligne, le contrôle de l'accès à certains services et données (pour les télétravailleurs, par exemple) et l'authentification des sites

  Web (pour les banques Internet, par exemple). L'authentification doit également inclure la possibilité de rester anonyme, dans la mesure où de nombreux services ne nécessitent pas l'identité de l'utilisateur, mais seulement la confirmation de certains critères (pièces justificatives anonymes), telle la capacité d payement.
- **Intégrité** – Confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées. Ceci est particulièrement important pour

l'authentification en vue de la conclusion de contrats ou quand l'exactitude des données est nécessaires (données médicales, design industriel, etc.…).

- **Confidentialité** – Protection des communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées. La confidentialité est particulièrement nécessaire pour la transmission des données sensibles et constitue une des exigences pour aborder les problèmes de protection de la vie privée des utilisateurs des réseaux de communication.

  Il convient de tenir compte de tous les événements qui menacent la sécurité et pas uniquement ceux de nature malveillante. Du point de vue d'un utilisateur, les menaces telles que les incidents environnementaux ou les erreurs humaines qui perturbent le réseau sont potentiellement aussi coûteuses que les attaques malveillantes**.** La sécurité des réseaux et de l'information peut donc être comprise comme la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, aux événements accidentels ou aux actions malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles.

I.12.Politique de sécurité

I.12.1.Définition

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité.

I.12.2.En quoi consistent les politiques de sécurité ?

Les politiques mises en œuvre doivent contrôler les accès à des zones définies du réseau et comment interdire l'accès à certaines zones à des utilisateurs non autorisés. Par exemple, seuls les membres du service des ressources humaines doivent avoir accès à l'historique des salaires des employés. Les mots de passe empêchent généralement les employés d'accéder aux zones protégées, mais à la condition que ceux-ci demeurent confidentiels. Des politiques écrites stipulant par exemple, que les employés ne doivent pas afficher leurs mots de passe sur leur bureau peuvent souvent prévenir certaines failles dans la sécurité.

Les clients ou fournisseurs ayant accès à certaines parties du réseau doivent également être l'objet de règles adéquates de ces politiques.

I.12.3. Qui doit appliquer et gérer ces politiques ?

La personne ou le groupe chargé de gérer et d'entretenir le réseau et sa sécurité doivent avoir accès à toutes ses zones.

La fonction de gestion des politiques de sécurité doit donc être confiée à des personnes particulièrement dignes de confiance et disposant des compétences techniques nécessaires.

Ainsi que nous l'avons mentionné auparavant, la plupart des failles dans la sécurité proviennent de l'intérieur, cette personne ou ce groupe ne doit donc pas constituer une menace potentielle. Une fois désignés, les gestionnaires du réseau bénéficient d'outils logiciels sophistiqués leur permettant de définir, de distribuer, de renforcer et d'évaluer les politiques de sécurité au moyen d'interfaces utilisant le modèle d'un navigateur Internet.

De définir les actions à entreprendre et les personnes à contacter on cas de détection de menace.

I.13.Type de menaces

Les menaces sont considérées comme une violation potentielle du système de sécurité elles viennent d'individus compétents à couse des vulnérabilités de système de sécurité.

En ce qui concerne l'analyse de risque, on a défini 12 types de menaces.

- Accidents physiques.
- Malveillance physique
- Panne du SI
- Carence de personnel.
- Interruption de fonctionnement du réseau.
- Erreur de saisie.
- Erreur de transmission.
- Erreur d'exploitation.
- Erreur de conception/ développement.
- **.**Copie illicite de logiciels.
- Indiscrétion/ détournement d'information

- Attaque logique

I.14.Classification des risques

I.14.1Les risques Humains

Les risques humains sont les plus importants, ils concernent les utilisateurs mais également les informaticiens.

- **Malveillances :** Certains utilisateurs peuvent volontairement mettre en danger le système d'information en y introduisant en connaissance de causes des virus, ou en introduisant
  Volontairement de mauvaises informations dans une base de données

- **Maladresse** : Comme en toute activité les humains commettent des erreurs, ils leur arrivent donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes.
- **Inconscience** : De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ils utilisent, et introduisent souvent des programmes malveillants sana le savoir.

- **Accidents :** il s'agit là d'un évènement perturbant les flux de données en l'absence de dommages aux équipements (panne, incendie, dégâts des eaux d'un serveur ou centre informatique,..).
- **Erreurs :** que ce soit une erreur de conception, de programmation de paramétrage ou de manipulation de données ou de leurs supports, l'erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisé des données.

I.14.2.Technique d'attaques par messagerie

En dehors de nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques tels que :

- **Le Pourriel (Spam) :** Un courrier électronique non sollicité, la plus part du temps de la publicité. Ils encombrent le réseau.
- **L'Hameçonnage :** un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles.

I.14.3.Attaques sur le réseau

Les principales techniques d'attaques sur le réseau sont :

- **Écoute (Le sniffing) :** L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent. De nombreux appareils du commerce facilitent les analyses et permettent notamment d'interpréter en temps réel les trames qui circulent sur un réseau informatique, Des protections physiques, pour les réseaux informatiques, ou le chiffrement (COMSEC, INFOSEC), pour tous types de réseau, offrent une protection adéquate pour faire face à ce type d'attaque.
- **La Mystification (Spoofing) :** technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles.

I.14.4.Agresseurs

Nous proposons les deux profils d'agresseurs les plus souvent identifiés :

- **Hacker ou passionné** : individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement et possède souvent un code d'honneur et de conduite. En général il n'a pas conscience de la mesure de ses actes. Comme mentionné plus haut dans le rapport [CERT-CC], l'agresseur passionné est de moins en moins expérimenté.
- **Cracker ou casseur :** plus dangereux que le *hacker*, cherche à nuire et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

I.14.5Cryptanalyse

L'attaque d'un chiffre ne peut se faire que lorsqu'on a accès aux cryptogrammes qui peuvent être interceptés lors d'une communication ou qui peuvent être pris sur un support quelconque. Cette attaque nécessite en général d'excellentes connaissances en mathématiques et une forte puissance de calcul, lorsqu'il s'agit d'algorithmes éprouvés, elle est principalement le fait de services de renseignement.

I.14.6.Un ver

Un ver est un programme malicieux qui a la faculté de se déplacer à travers un réseau qu'il cherche à perturber en le rendant indisponible. Cette technique de propagation peut aussi être utilisée pour acquérir des informations par sondage.

Par exemple, le ver MS-SQL Slammer, qui le 25 janvier 2003 a provoqué une augmentation du trafic Internet telle qu'elle a ralenti, voire bloqué de manière perceptible, une partie des SI mondiaux.

Aujourd'hui ces deux derniers types d'attaque que sont les "Vers" et "Virus" se rapprochent, tel qu'il devient difficile d'en faire une distinction nette.

Parmi les plus célèbres nous pouvons citer :

- Code Red, apparu en août 2001, profitait d'une faille de certains serveurs web pour se propager,
- Nimda, apparu en septembre 2001, a utilisé plusieurs techniques de propagation pour infecter les systèmes et en laissant derrière lui des portes dérobées sur ces systèmes.

I.14.7.Virus

Nommé ainsi parce qu'il possède de nombreuses similitudes avec ceux qui attaquent le corps humain, un virus est un programme malicieux capable de se reproduire et qui comporte des fonctions nuisibles pour le SI : on parle d'infection. Le virus dispose de fonctions qui lui permettent de tester s'il a déjà contaminé un programme, de se propager en se recopiant sur un programme et de se déclencher comme une bombe logique quand un événement se produit. Ses actions ont généralement comme conséquence la perte d'intégrité des informations d'un SI et/ou une dégradation ou une interruption du service fourni.

I.14.8.Cheval de Troie

Subterfuge employé par les Grecs pour prendre Troie, en informatique un cheval de Troie est un programme ou un fichier qui comporte une fonctionnalité cachée connue de l'attaquant seul. Elle lui permet de contourner des contrôles de sécurité en vigueur. Cependant un cheval de Troie doit d'abord être installé et ceci n'est possible que si les mesures de sécurité sont incomplètes, inefficaces ou si l'agresseur bénéficie d'une complicité.

Un cheval de Troie doit être attirant (nom évocateur) pour être utilisé, posséder l'apparence d'un authentique programme (un utilitaire par exemple) pour inspirer confiance et

enfin ne pas laisser de traces pour ne pas être détecté. La simulation de terminal, dont le but est de s'emparer du mot de passer d'un utilisateur, est un cheval de Troie.

En conséquence, identifier la présence d'un cheval de Troie n'est pas aisée et une bonne connaissance du système et des applications installées est nécessaire.

I.14.9.Logiciel espion (spyware)[4]

Un logiciel espion est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de transmettre à des tiers des informations de l'environnement sur lequel il est installé sans que l'utilisateur n'en ait conscience.

I.14.11.LES menaces intentionnelles

Une menace intentionnelle est une action exécutée par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources.

I.14.12Les menaces accidentelles

Les menaces accidentelles peuvent se manifester ou résulter de l'exposition ou de la modification d'un objet, elles être des erreurs des utilisateurs ou d'administrateurs, matériel ou accidents de nature industrielle.

I.15.Les protocoles de sécurité

- **Protocole SSL**

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.….).

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

1. Le navigateur du client fait une demande de transaction sécurisée au serveur.

2. Suite à la requête du client, le serveur envoie son certificat au client.

3. Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.

4. Le client choisit l'algorithme.

5. Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.

6. Le navigateur vérifie que le certificat délivré est valide.

7. Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

Afin d'éviter des attaques, il est recommandé d'utiliser la double authentification c'est-à-dire non seulement l'authentification du serveur mais également celle du client, bien que l'authentification du client avec SSL soit facultative.

- **Le protocole SSH**

Le protocole SSH (Secure Shell) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

- **Le protocole HTTP**

S-HTTP (Secure HTTP) est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP. Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle.

- **Fonctionnement de S-HTTP:**

Contrairement à SSL qui travaille au niveau de la couche de transport, S-HTTP procure une sécurité basée sur des messages au-dessus du protocole HTTP, en marquant

individuellement les documents HTML à l'aide de "certificats". Ainsi, alors que SSL est indépendant de l'application utilisée et crypte l'intégralité de la communication, S-HTTP est très fortement lié au protocole HTTP et crypte individuellement chaque message.

Les messages S-HTTP sont basés sur trois composantes:

- Le message HTTP
- Les préférences cryptographiques de l'envoyeur
- Les préférences du destinataire

Ainsi, pour décrypter un message S-HTTP, le destinataire du message analyse les en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message. Puis, grâce à ses préférences cryptographiques actuelles et précédentes, ainsi que des préférences cryptographiques précédentes de l'expéditeur, il est capable de décrypter le message.

- **Le protocole IP sec**

IPSEC fournit trois principaux mécanismes de sécurité :

- **Confidentialité et protection contre l'analyse du trafic *:***

Les données transportées ne peuvent être lues par un adversaire espionnant les communications. En particulier, aucun mot de passe, aucune information confidentielle ne circule en clair sur le réseau. Il est même possible, dans certains cas, de chiffrer les en-têtes des paquets IP et ainsi masquer, par exemple, les adresses source et destination réelles. On parle alors de protection contre l'analyse du trafic.

- **Authenticité des données et contrôle d'accès continu**

L'authenticité est composée de deux services, généralement fournis conjointement par un même mécanisme : l'authentification de l'origine des données et l'intégrité.

L'authentification de l'origine des données garantit que les données reçues proviennent de l'expéditeur déclaré.

L'intégrité garantit qu'elles n'ont pas été modifiées durant leur transfert. La garantie de l'authenticité de chaque paquet reçu permet de mettre en œuvre un contrôle d'accès fort tout au long d'une communication, contrairement à un contrôle d'accès simple à l'ouverture de la connexion qui n'empêche pas un adversaire de récupérer une communication à son compte,ce service permet en particulier de protéger l'accès à des ressources ou données privées.

- **Protection contre le rejeu**

La protection contre le rejeu permet de détecter une tentative d'attaque consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau.

I.16.LES méthodes de protection

I.16.1.Logiciels antivirus

La plupart des ordinateurs sont dotés d'un logiciel antivirus pré intégré capable de détecter les principales menaces virales s'il est régulièrement mis à jour et correctement entretenu.

Avec des milliers de nouveaux virus générés chaque mois, il est crucial que la base de données des virus soit tenue à jour. La base de données des virus est l'enregistrement du logiciel d'antivirus qui permet d'identifier les virus connus lorsqu'ils surviennent.

La politique de sécurité du réseau doit mentionner que tous les ordinateurs du réseau doivent être tenus à jour et théoriquement qu'ils doivent tous être protégés par le même système d'antivirus (entre autres, afin de réduire au maximum les frais de maintenance et de mise à jour).

I.16.2Le chiffrement

Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message, Ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur L'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique.

- **Le cryptage symétrique**

Le cryptage à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard) et RSA.

Le principal problème est le partage de la clé : Comment une clé utilisée pour sécuriser peut être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : Key management) limite les systèmes des clés privées surtout sur Internet.

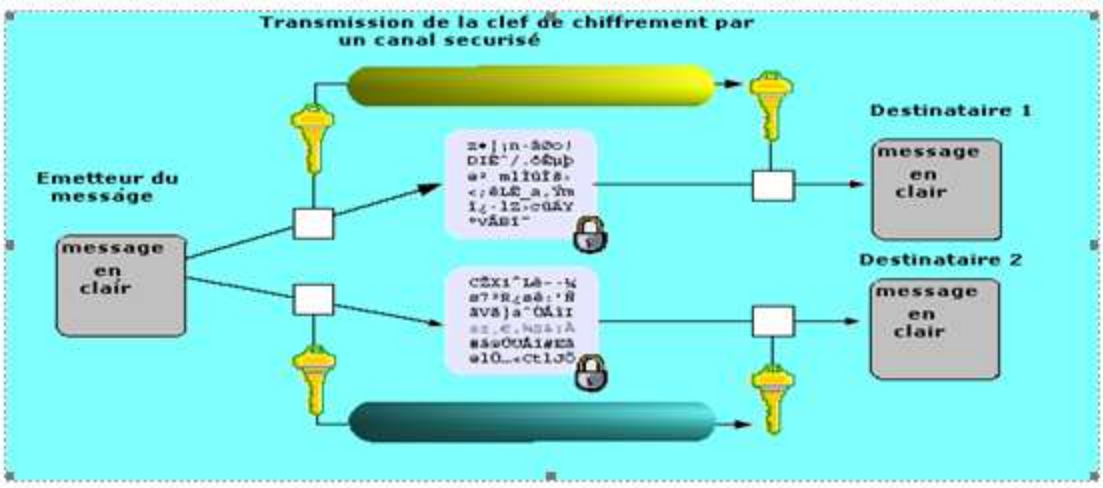


Figure I. 8:Cryptage Symétrique

- **Le cryptage asymétrique**

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Ce cryptage présente l'avantage de permettre le placement des signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- Authentification plus flexible.
- Supporte les signatures numériques.

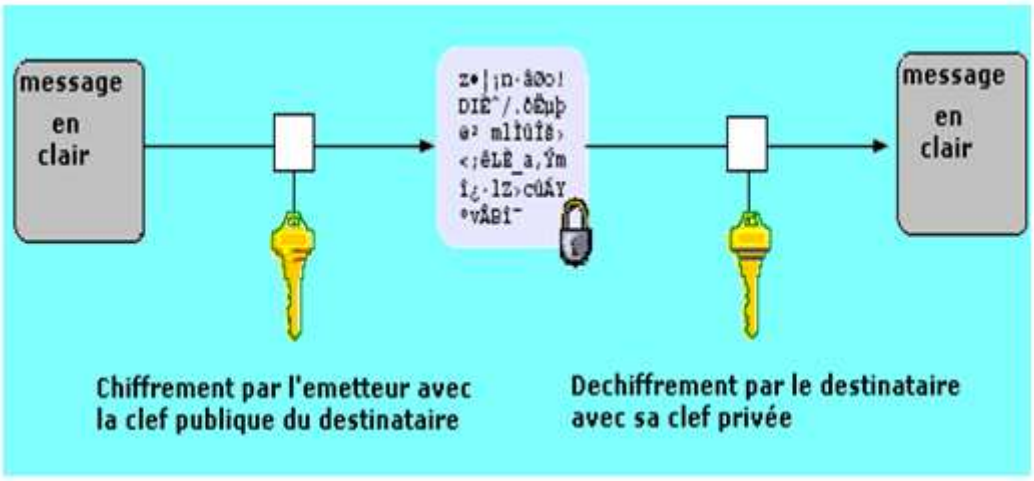


Figure I. 9: Cryptage asymétrique

I.16.3.L'Authentification

I.16.2.1.Introduction

L'Authentification est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé**.**

La combinaison de plusieurs de ces méthodes (aussi appelées facteurs d'authentification) permet de renforcer le processus d'authentification, on parle alors d'authentification forte.

Les techniques d'authentification les plus usitées sont, de loin, les mots de passe mais aussi, de plus en plus, les Certificats de clés publiques**.**

I.16.2.2.Mots de passe

Le moyen le plus simple et le plus classique de s'assurer que seules les personnes autorisées peuvent accéder à une certaine partie du réseau est de protéger certaines zones du réseau par un mot de passe.

De nombreux utilisateurs choisissent des chiffres ou des mots faciles à retenir pour leurs mots de passe, comme des dates d'anniversaires, des numéros de téléphone ou des noms d'animaux de compagnie, d'autres ne changent jamais leurs mots de passe et ne se soucient pas de leur confidentialité.

I.16.3.Certificats numériques

Les certificats numériques sont généralement utilisés à des fins d'identification, lors de l'établissement de tunnels sécurisés sur Internet, comme c'est le cas dans les réseaux virtuels privés (VPN) et sont émis par une autorité de certification.

I.16.4.Système de détection d'intrusions

Un système de détection d'intrusions reposant sur le réseau fournit une surveillance constante du réseau. Ce système analyse les flux de paquets de données du réseau à la recherche d'activités non autorisées, telles que les attaques de pirates, et permet aux utilisateurs de répondre aux failles dans la sécurité avant que les systèmes ne soient compromis.

Dans l'illustration suivante un système de détection d'intrusions est comparé à une caméra vidéo et à un détecteur de mouvement repérant les activités non autorisées ou douteuses et travaillant avec des systèmes de réponse automatisée tels que les surveillants, pour interrompre l'activité.

I.16.5.L'audit de sécurité informatique

C'est l'opération d'évaluation et de contrôle des moyens de prévention et de protection des risques informatiques.

I.17.Pare feu : pare-feu

I.17.1Introduction

Si nous devions classer les outils disponibles à l'heure actuelle pour améliorer la sécurité d'un réseau en fonction de leur succès, les pare-feu remporteraient sans aucun doute la première place. En effet, de plus en plus des sociétés ont proposées des «solutions firewall» puissantes, qui ont de plus l'avantage d'être quasiment complètes.

De plus, ce terme semble être petit à petit rentré dans les habitudes concernant la sécurité réseau. Mais que signifie exactement le terme « pare-feu» ?

En fait, le mot pare-feu souvent utilisé un peu abusivement, signifie qu'on instaure une série de protections en un point particulier entre deux entités connectées.

L'occurrence entre Internet et le réseau interne d'une entreprise. En pratique, le pare-feu consistera donc en une architecture, plutôt qu'un matériel ou un logiciel précis. Cette architecture intégrera alors Une série de composants matériels et logiciels qui eux tenteront précisément d'assurer le Niveau de sécurité requis.

L'architecture la plus en vogue actuellement est basée sur une « zone démilitarisée» Communément appelée DMZ (Demilitarized zone).

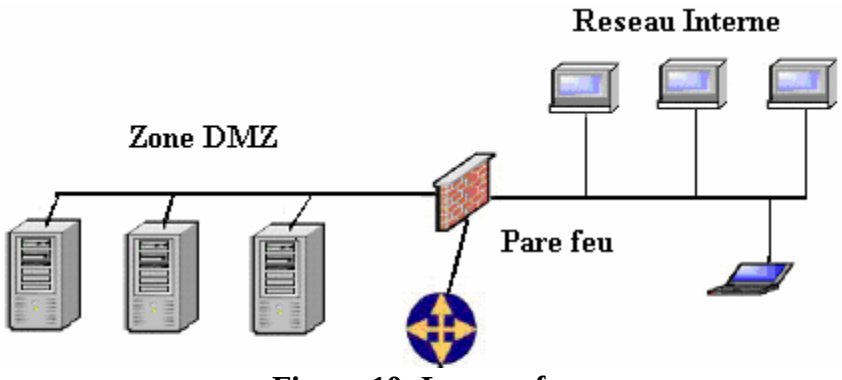


Figure 10: Le pare feu

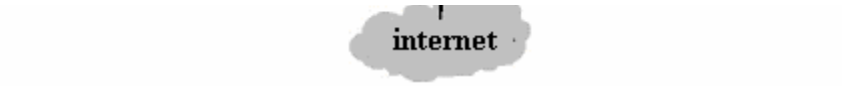


Figure I.10: Par feu

Elle consiste à placer un réseau Intermédiaire entre l'accès Internet et le réseau interne (éventuellement plusieurs). Cette DMZ sera isolée, aussi bien vis à vis de l'Internet que du réseau local, par des systèmes de filtrage (filtres de paquets). Ensuite, les éventuels serveurs nécessaires à l'entreprise devant continuer à être accessibles de l'extérieur seront connectés directement sur cette DMZ, de manière à les séparer du réseau interne, Par exemple, on pourra y trouver un serveur Web, un serveur DNS, un serveur de mails, un serveur FTP...

Dans le cas où l'un de ces serveurs serait compromis, le filtrage entre la DMZ et le réseau interne doit être capable en plus d'assurer une protection suffisante.

Bien évidemment, cette architecture doit être adaptée plus précisément à la structure d'une entreprise précise, et éventuellement intégrer des composants supplémentaires, tels que des proxys et autres dispositifs.

I.18.Les VPN

VPN (Virtual Private Network) ou RPV (Réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique.

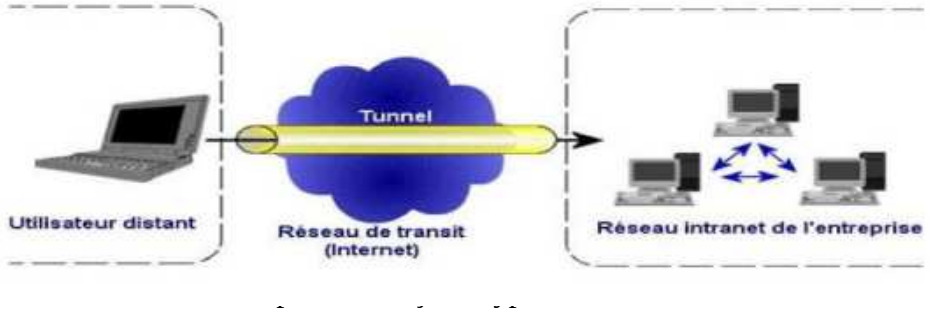


Figure I. 11:Réseau privé virtuel

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets de l'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé, comme Internet.

I.18.1.Les différents types de VPN

Selon les besoins, on distingue trois types de VPN :

- **Le VPN d'accès**: il est utilisé pour permettre à des utilisateurs nomades d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.
- **L'intranet VPN** : il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants .Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants).
- **L'extranet VPN:** une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

I.19.Les VLAN

Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.

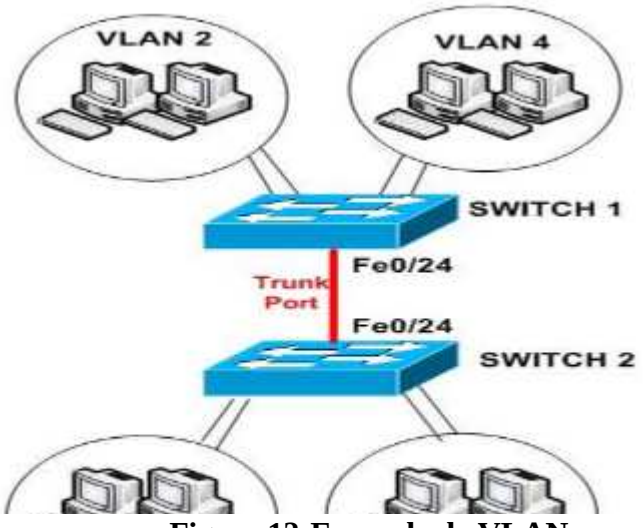


Figure 12:Exemple de VLAN

Figure I.12:VLAN

I.19.1Les différents types de VLAN

Pour répondre aux objectifs des VLAN, la règle suivante doit être impérativement respectée, une trame doit être associée à un VLAN et un seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respectée.

Les méthodes de construction d'un VLAN doivent donc déterminer la façon dont le commutateur va associer la trame à un VLAN. Usuellement on présente trois méthodes pour créer des VLAN : les vlan par port (niveau 1), les Vlan par adresses MAC (niveau 2), les VLAN par adresses IP (niveau 3) ainsi que des méthodes dérivées.

- **Les VLAN par port (Vlan de niveau 1)** : chaque port des commutateurs est affecté à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. Si une station est physiquement déplacée, il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon Vlan. Si une station est logiquement déplacée, il faut modifier l'affectation du port au Vlan.

- **Les Vlan par adresse MAC (Vlan de niveau 2**) : chaque adresse MAC est affectée à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En effet il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapter à l'utilisation de machines portables). Si on veut changer de Vlan il faut modifier l'association Mac / Vlan. Les Vlan par adresse de Niveau 3 (VLAN de niveau 3): une adresse IP est affectée à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par

son adresse IP .En effet, il s'agit à partir de l'association adresse IP/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2. Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.

I.20.LES services réseaux

I.20.1.Serveur WEB (http)

Est un logiciel capable d'interpréter les requêtes http qu'il reçoit et fournit une réponse dans ce même protocole .Apache est le serveur http le plus répondu sur internet. Ce dernier, permet en effet d'ajouter des modules supplémentaires qui enrichissent le serveur en termes de fonctionnalités

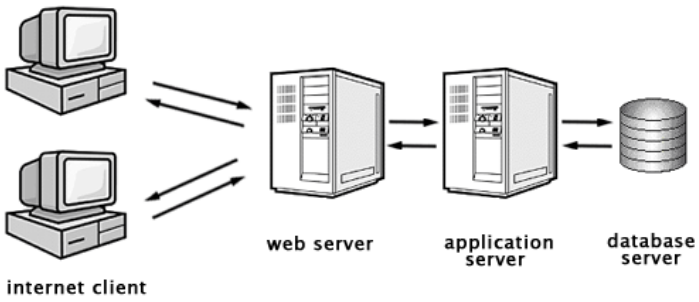


Figure I.13: Serveur Web

I.20.2.Le serveur DNC

LE service DNC signifiant Domain Name service est né de la volonté de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatique tels que l'internet.

Les machines ne sachant communiquer qu'à travers l'échange d'adresses IP difficiles à mémoriser pour l'homme, le DNS agit comme un annuaire téléphonique en fournissant la correspondance entre le nom de la machine et son adresse IP. Ainsi, lorsque l'on veut se

connecter à un ordinateur dont on connait le nom d'hôte, on interroge un serveur DNS qui nous renvoie l'adresse IP correspondant à ce nom.

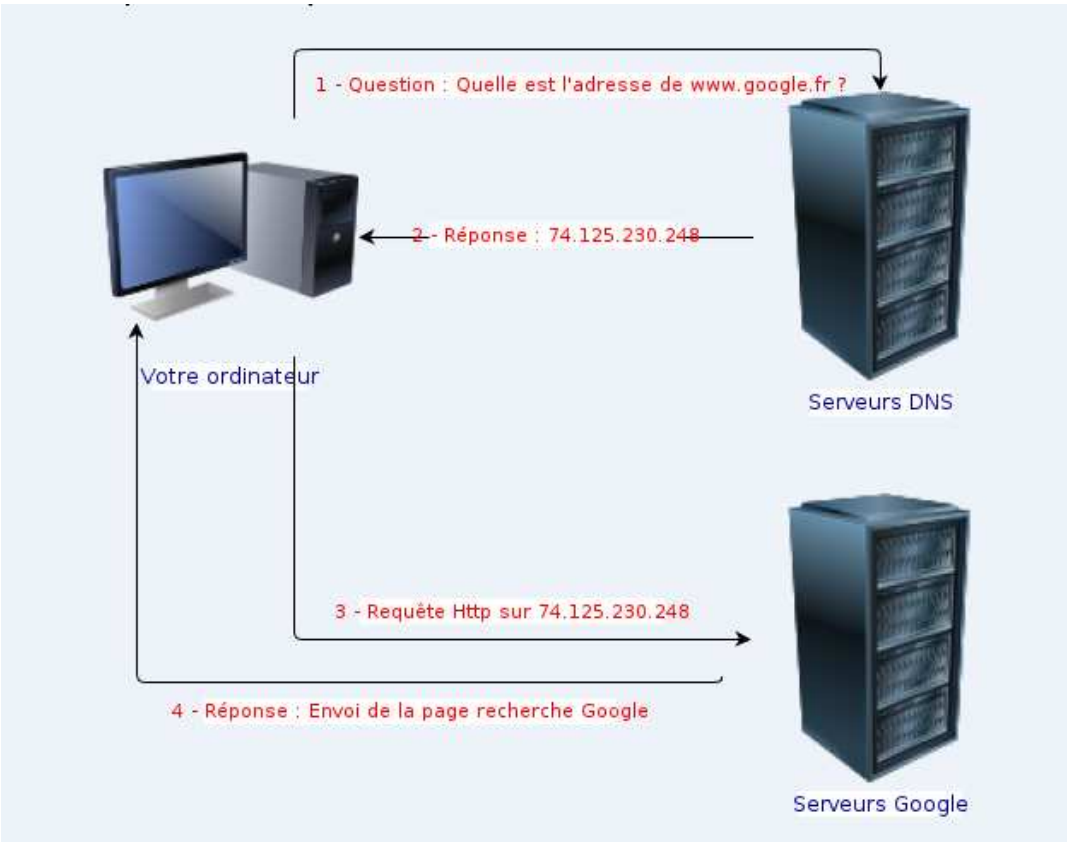
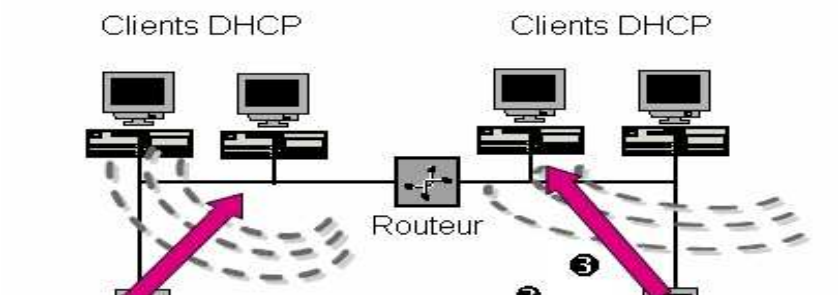


Figure I.14: Serveur DNS

I.20.3.Le serveur DHCP

Le serveur DHCP signifie dynamic host configuration protocole et désigne un prot s IP d'une se de broad faut.



I.20.3.Le serveur Proxy

Le serveur Proxy (appelé aussi serveur mandataire) et un serveur recevant des requêtes qui ne lui sont pas destinées et qui les transmet aux autres serveurs. Quand il reçoit une requête, le serveur proxy stocke le résultat. Si la même requête lui est à nouveau envoyée, il vérifie que le résultat n'a pas été modifié et renvoie le résultat qu'il a " déjà sous la main " à celui qui a fait la requête (fonctionnant ainsi comme un cache), c'est la mise en cache des URL et des objets résultant du surf. Le but est d'améliorer (point de vue vitesse) le surf.

La plupart des proxys permettent également de faire du filtrage de contenu (blacklist), c'est à dire d'autoriser ou d'interdire l'accès à certains sites qui peuvent contenir des informations non désirées pour certains publics (pornographie, violence, haine racial, etc. ….).

Il existe plusieurs serveur Proxy fonctionnent sur différente plate-forme (Microsoft, Linux Mac OS). Certain sont gratuits et d'autres payant.

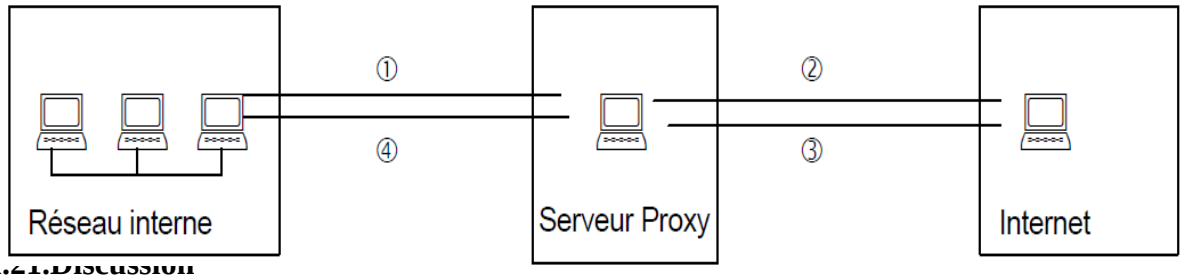


Figure I.16: Le serveur proxy

I.21.Discussion

Les technologies Internet amènent ces dernières à se confronter à différents degrés de vulnérabilités qui sont loin d'être négligeables.

La maitrise des nouvelles technologies par le grand public engendre un accroissement des menaces et une diversification d'outils d'attaques qui ne cessent de se perfectionner.

Dans ce chapitre nous avons présenté des généralités sur les réseaux informatiques. Vu la fiabilité de communication qu'ils assurent, ils sont devenus aujourd'hui une nécessité dans le monde de travail. Les différentes menaces et attaques sur divers systèmes nous ont ramené à parler de la nécessité de garantir certains besoins de sécurisation : tels que l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que les méthodes d'attaques et comment se protéger contre elles.

Dans le deuxième chapitre nous allons présenter le cas d'une entreprise dépourvue d'une DMZ et la solution que nous lui proposerons pour améliorer et augmenter le niveau de sécurité de son réseau.

II.1.Préambule

Un réseau est soumis régulièrement à de nombreuses évolution et modifications avec le développement de la technologie et le besoin de sécurité qui l'accompagne.

Le but de ce chapitre est de présenter un plan de sécurité pour l'applique au niveau du réseau de l'entreprise de l'entreprise. Nous allons présenter le réseau existant et ses critiques ainsi que Les services de sécurités adaptatifs Cisco ASA qui permet aux administrateurs de mieux segmenter le trafic réseau et de créer des zones de sécurité séparées.

II.2.Approches du travail

1. Etude bibliographique

- Recherche d'informations sur les menaces informatiques, les failles de sécurité des équipements et les protocoles réseaux et les différentes techniques et outils d'attaques afin d'avoir une meilleure idée sur les procédures à appliquer.

2. Etude théorique

- Etudier les matériels et leur configuration,
- Etudier les attaques possibles ciblant ces équipements,
- Rechercher un simulateur réseau.

3. Etude d'ingénierie

- Gestion et réalisation du projet : Maîtrise d'ouvrage et maîtrise d'œuvre
- Rédaction des procédures correspondantes aux choix techniques et fonctionnels
- Exploitation des bases scientifiques pour comprendre le mécanisme des attaques pour pouvoir appliquer les procédures de sécurité.

4. Réalisation :

- Manipulation des configurations du matériels et application des procédures de sécurité afin d'établir les règles de protection nécessaires.

II.3.Présentation de l'entreprise

L'offre du 2int (Institut International des nouvelles Technologies) est centrée sur les systèmes et réseaux, le développement d'application, les bases de données et les environnements « Open Source ». Sans oublier les formations certifiantes (Cisco, Microsoft,….) pour les utilisateurs spécifiques autour des applications bureautiques et de travail collaboratif.

Le groupe 2int a bâti un savoir-faire et une expérience, au service de ses clients. Des centaines d'organisation s'appuient sur 2intPartners.

2intPartners déploie des services de vente, d'installation, de gestion et de maintenance de matériel informatique et de réseau, L'offre se complète de logiciels de sécurité et de bureautique, incluant (Antivirus, licence Microsoft,etc.…)

II.4.Architecteur d'organisme d'accueil

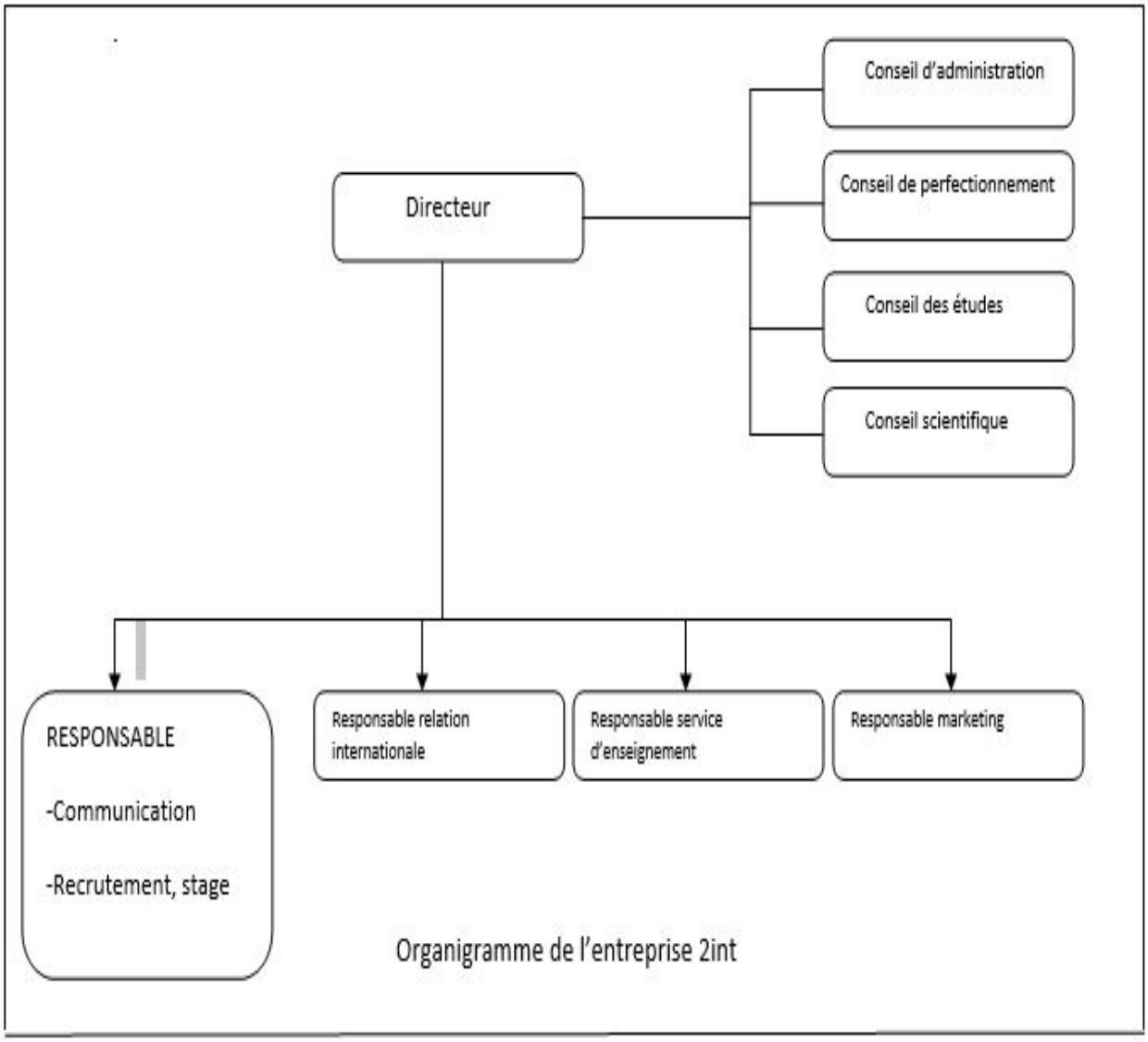


Figure II. 1: Organigramme de l'entreprise 2int

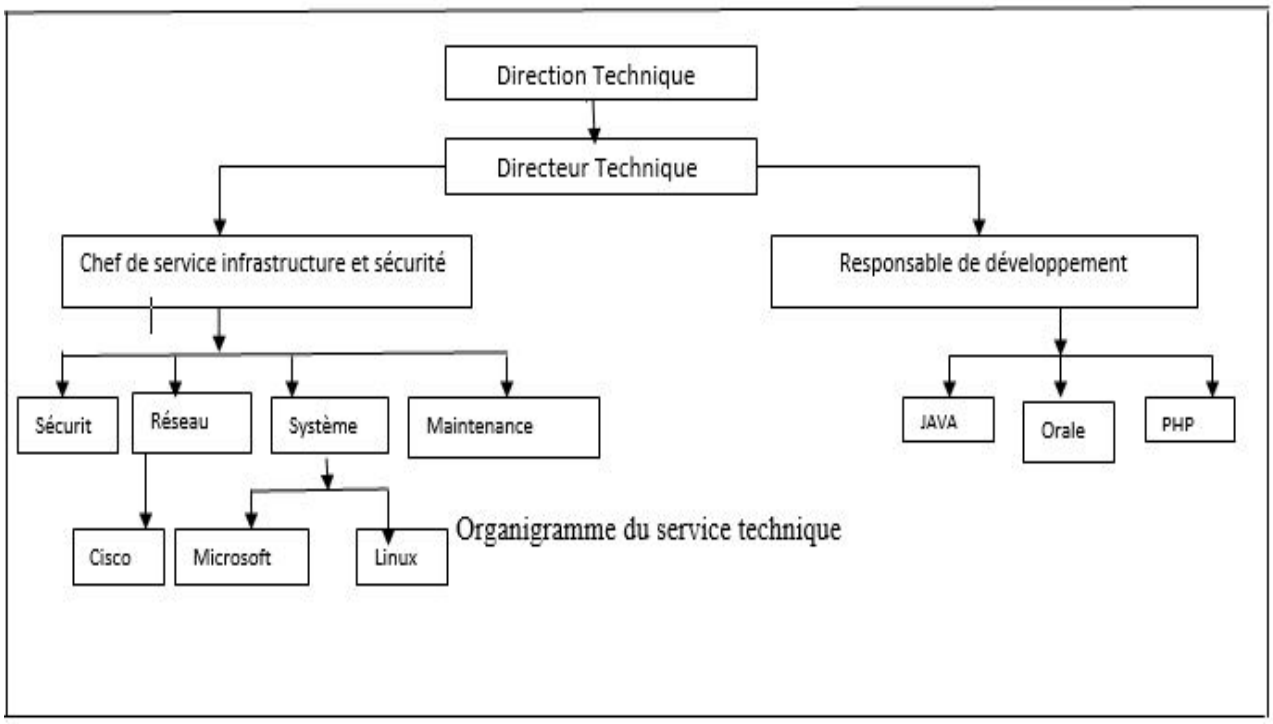


Figure II. 2:Organigramme du service technique

II.5. Architecteur du réseau d'entreprise existant

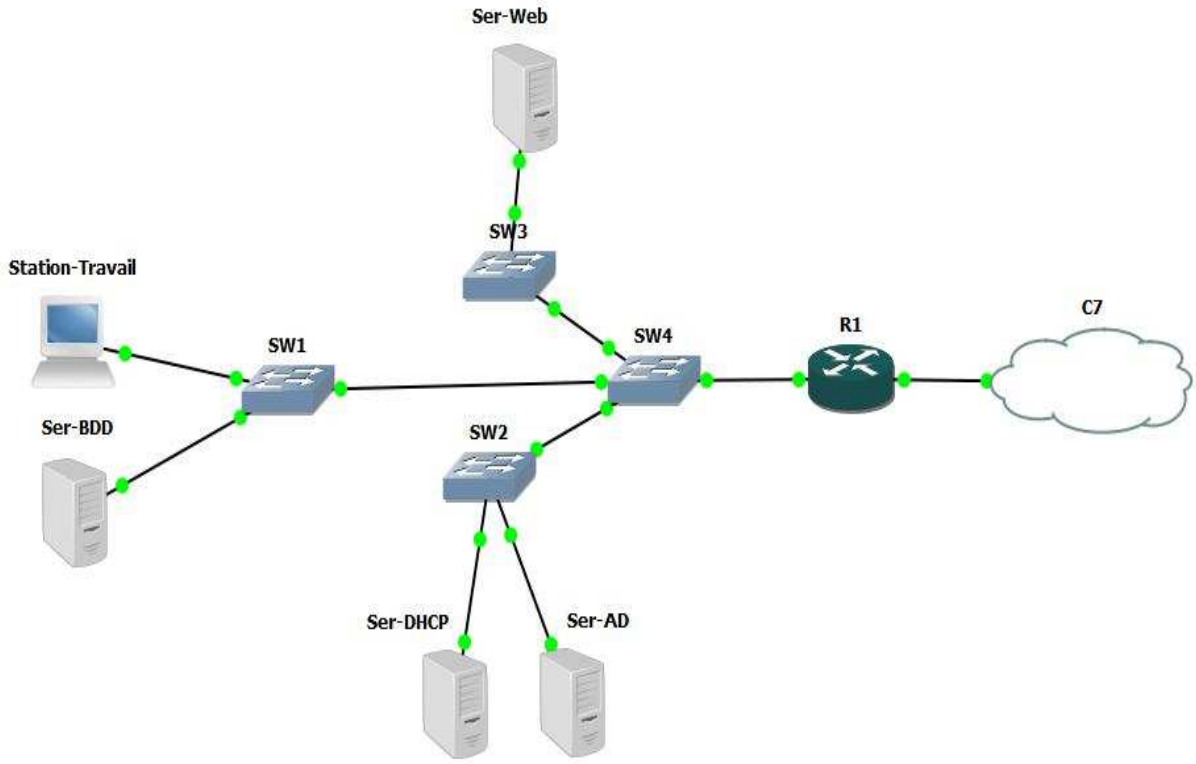


Figure II. 3:Architecture du réseau existant

II.5.Les Critiques du réseau existant

Critique 1 : Le réseau est installé anarchiquement et non administré.

Critique 2 : Le réseau n'est pas sécurisé il est disposé au réseau externe (internet).

Critique 3 : Le réseau installé est non sécurisé contre les intrusions d'une façon faible.

Critique 4 : L'accès est permis de chaque unité émettrice vers n'importe quelle unité destinataire (accès non limité).

Critique5 : L'absence de gestion réseaux centralisé « Domain » (tous les machines interconnectes elles sont dans le même groupe de travaille

Critique 6 : L'absence de VLANs (augmentation du trafic réseau)

Critique7 : Le serveur DHCP ne pas sécuriser (les attaques de « DHCP spoofing »)

Critique 8 : Manques firewall pour sécuriser l'accès (DMZ, ACL, zone base firewall)

Critique9 : Manque de VPN pour les connexions nomades

Critique10 : Manque de politique de cryptage de données l'intégrité des données

Critique11 : Manque de stratégie de gestion d'autorisation pour assure la disponibilité des données

Critique12 : Manque de serveur radius pour l'authentification

Critique13 : Le manque de sécurité au niveau de port de Switch (les attaques par « mac flooding » et les attaques « man in the middle »

Critique14 : Manque d'un système de détection d'intrusion pour analyser le contenu des paquets (Données)

II.6.Solution proposées

A l'issu d'une préalable de réseau existant nous avons opté pour l'implémentation du plans de sécurité suivant :

- Administration et ordonnancement du réseau local.
- Configuration d'un firewall(ASA 5510)
- Isolation des postes à l'aide de VLAN (pour segmenté les réseaux et minimisé le trafic réseau)
- Installation d'un serveur radius (pour l'authentification)

L'architecteur du réseau avec les solutions proposées dans ce plan de sécurité est par la figure

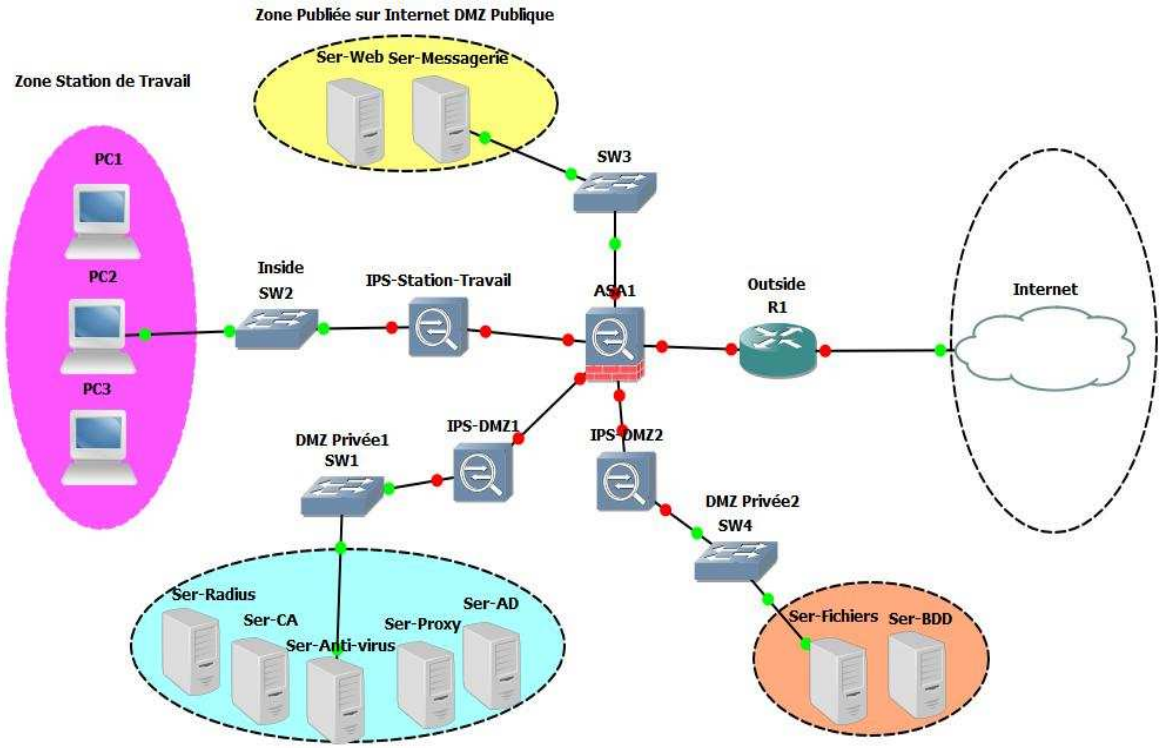


Figure II. 4:Architecteur du réseau proposé

Ce modèle est constitué de cinq grandes parties qui sont les suivantes :

1 Extérieur : Cette partie concerne toutes les entités qui sont à l'extérieur de l'entreprise. Ces entités peuvent être des commerciaux nomades qui transmettent leurs données, des employés qui veulent avoir accès à leurs comptes, des internautes voulant naviguer sur le site institutionnel de l'entreprise ou des partenaires commerciaux qui veulent faire des échanges à travers l'Extranet de l'entreprise.

2DMZ Publique : Cette partie de l'architecture contiendra les serveurs et les services accessibles de l'extérieur et de l'intérieur. On trouvera par exemple le serveur Web, le serveur de messagerie, qui sont publiés (exposé) sur internet d'une façon sécurisée.

- Serveur web : Pour la publication (exposé) d'une façon sécurisée sur internet.
- Serveur de messagerie : Pour la publication (exposé) d'une façon sécurisée sur internet.

3 DMZ Privée1 (Gestion de sécurité) : Cette DMZ est plus sécurisée que la DMZ Publique. Elle sera seulement accessible à partir du réseau Interne et d'internet via les VPN, Cettepartie contiendra les serveurs (Radius, Active Directory,Admin KitKaspersky, autorité de certifications, DHCP, proxy-cache) des utilisateurs.

- Serveur Radius : Pour gestion centralisée (Authentication, Autorization and Accounting)
- Serveur des certificats d'autorité : Pour la gestion des Clefs publiques et privées (La cryptographie asymétrique) pour assurer l'intégrité des données.
- Serveur d'Active Directory : Pour gestion des objets (Utilisateurs, PCs, Imprimantes, ... etc.).
- Serveur DHCP : l'allocation des adresses IP automatique pour les postes clients.
- Serveur Proxy : Sauf les machines qui ont le proxy qui peuvent se connecter à internet.

4 DMZ Privée2(Stockage) : Cette DMZ est utilisée pour la gestion de stockages des données (Serveurs de BDD, Serveur de fichiers).

- Serveur de Base de données : gestion de la BDD.
- Serveur de fichiers : gestion des fichiers.

5 Réseau Interne : Cette partie regroupera les différents utilisateurs de l'entreprise. Elle doit être la plus sécurisée des différentes autres parties. C'est pour cela qu'elle n'est pas accessible de l'extérieur. [9]

Matériels à utiliser

Lors de la conception de l'architecture réseau proposée nous avons utilisé plusieurs matériels afin d'aboutir à un bon résultat et voici la liste des matériels utilisés:

- Serveur de certificats d'autorités.
- Serveur d'authentification Radius.
- Serveur DHCP.
- Serveur Web.
- Serveur de messagerie.
- Serveur d'Active Directory (Windows Serveur 2012).
- Serveur de Base de données.
- Serveur de fichiers.
- Des postes client
- Des Switch Cisco
- Un routeur
- Un firewall ASA
- Câbles de connexions.

Logiciel à utiliser

- Dans les postes serveur (Windows server 2012)
- Dans les postes client (Windows 7)

II.7.Présentation du matériel

II.7.1.Les Routeurs Cisco

La fonction principale d'un routeur Cisco consiste à diriger les paquets destinés à des réseaux locaux et distants en :

- Déterminant le meilleur chemin pour l'envoi des paquets.
- Transférant les paquets vers leur destination.

II.7.2.Les Switch Cisco(CATALYST cisco)

Les commutateurs intelligents Cisco Catalyst, nouvelles famille de périphérique autonomes à configuration fixe, apportent au poste de travail une connectivité Faste Ethernet et gigabit Ethernet optimisent les services de LAN sur les réseaux d'entreprise. [10]

- **Ces caractéristiques sont :**

Fonctionnalités intelligentes à la périphérie du réseau, par exempledes listes de contrôle d'accès (ACL) élaborées et une sécurité optimisée.

Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.

II.8.Présentation des logicielles

II.8.1.Windows server 2012

Microsoft Windows Server 2012 est conçu pour fournir aux entreprises la plate-forme la plus productive pour virtualiser les charges de travail en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web.

FigureII. 5: server Windows 2012

II.8.2.Le simulateur graphique de réseaux

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 (Graphical Network Simulateur). Un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel.

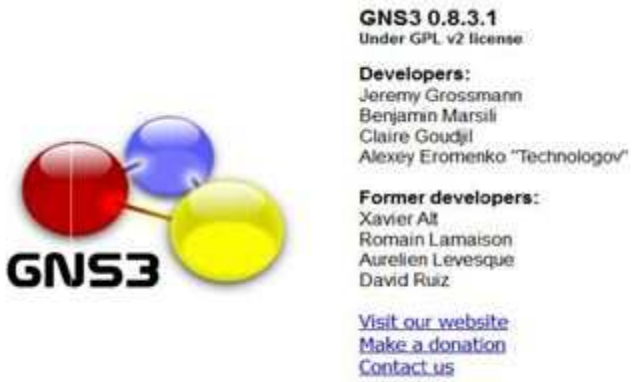


Figure II. 6:GNS3

II.8.3.La VMware Workstation 10

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web

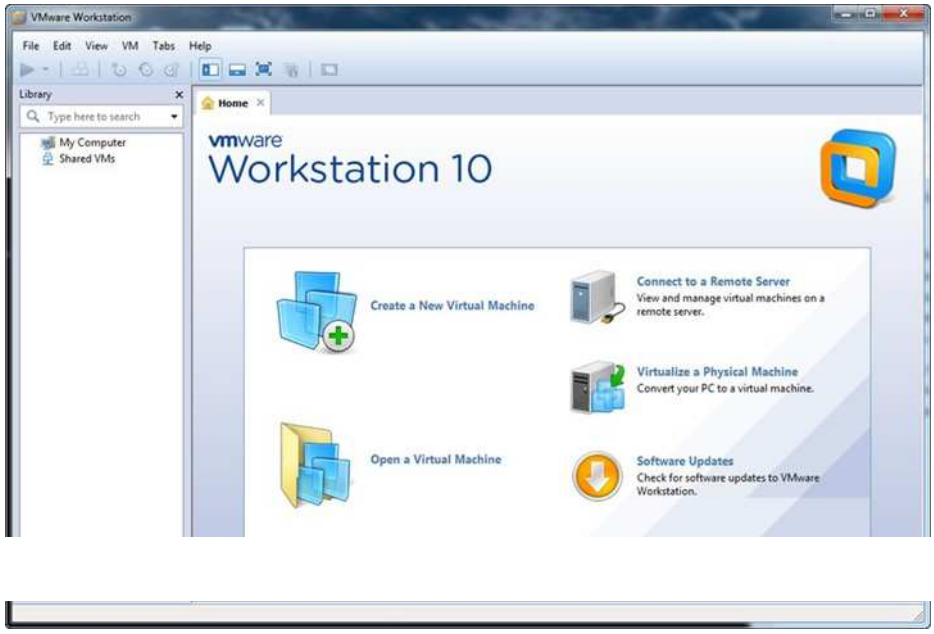


Figure II. 7: VMware Workstation 10

II.8.4.Active Directory

Active directory est le nom de service d'annuaire (au sens informatique) de Microsoft. AD permet de regroupe toutes les informations concernant le réseau que ce soient utilisateur, les machines ou les applications. L'utilisateur peut ainsi trouver facilement des ressources partages et les administrations peuvent contrôle leurs utilisation grâce à des fonctionnalités de sécurisation des accès aux ressources répertoriées. AD a pour objectif de permettre la gestion des comptes, des ordinateurs, des ressources et de la sécurité de façon centralisée, dans le cadre d'un domaine.

Figure II. 8:Active directory

II.8.4.1.Le service de domaine Active Directory (AD DS)

Les services de domaine Active Directory fournissent les fonctionnalités d'une solution de gestion des identités et des accès (IDA :Identity and Access) pour les réseaux d'entreprise sous Windows.

IDA est nécessaire pour maintenir la sécurité des ressources d'une entreprise tel que : fichiers, messages électronique, application et base de données.

Une infrastructure doit assurerLes fonctionnalités suivantes :

- Mémoriser les informations sur les utilisateurs, les groupes et les autres identités.
- Authentifier une identité.

- Contrôle d'accès.
- Fournir une trace d'audit.

II.9.Serveur de fichier

Un serveur de fichier fournit un emplacement central sur votre réseau ou vous pouvez stocker des ressources (fichiers) et les partager avec des utilisateurs de votre réseau.
Lorsque les utilisateurs ont besoin d'un fichier important qui doit être accessible pour un grand nombre de personnes, ils prouvent accéder à distance au fichier situé sur le serveur de fichier au lieu de transférer le fichier entre les ordinateur individuels.[11]
On utilise généralement l'un des quatre protocoles suivants :

- FTP (File Transfert Protocol)
- CIFS (Common Internet File System) anciennement nommé SMB (Server Message Block)
- NFS (Network File System)
- NCP (Netware Core Protocol)

Le choix de protocole dépond principalement de la méthode d'accès des utilisateurs. CIFS est utilisé par le système d'exploitation Microsoft Windows, NFS est répondu dans le milieu UNIX. Tout fois des implémentations de ces protocoles sont disponibles pour tout type de système. Ces deux protocole permettent d'établir des liaisons, permanentes enter le client et l serveur.

II.9.1.Installation de serveur de fichier

Windows server 2012simplifie les taches de création, de partager et d'administration en regroupant toutes les fonctionnalités du serveur de fichier autour d'un seul et même rôle.
Il existe trois types de partage de fichier sur Windows : SMB, NFS et DFS.

- SMB est un partage qui fonctionne avec tous les autres systèmes d'exploitation MAC OS X et Linux.
- NFS quant à lui, est exclusivement utilisé pour partager des fichiers entre machines Windows et UNIX.

DFS permet de faire du partager de fichier via un unique espace de noms les utilisateurs n'ont plus à se soucier du nom du serveur mais juste d'un espace de nom DFS permet aussi de faire de la redondance en faisant de la réplication.

II.10.Serveur web

Les sites web permettent d'accéder à des bases de données dans des environnements publics et intranet et autorisent une certaine personnalisation en fonction de besoins particuliers. Les applications ou les services Web se basent sur divers normes, protocoles et technologies de développement.

Le système d'exploitation Windows server 2012 inclut IIS7.0 (Internet Information Services), une plate-forme de services web complet capable de prendre en charge plusieurs types de contenu et d'application web. IIS7.0 propose des nettes améliorations au niveau de la gestion de l'extensibilité et de fiabilité. Elle assure également une rétrocompatibilité pour supporter les millions des sites Web déjà hébergés sur les versions précédentes d'IIS.

II.10.1.Cas d'utilisation des serveurs Web

Le principal avantage d'utiliser du contenu et des applications Web est l'accessibilité depuis une large gamme d'ordinateurs clients.

La plate-forme IIS a été conçue pour prendre en charger une variété de scénarios .en voici quelques exemples :

- Sites web publics : la plupart ont des besoins relatives simples pour communique des informations sur internet.
- achats en linge : internet est devenu un centre commercial qui permet aux vendeurs d'afficher et de vendre une grande variété de produits.
- Intranet : le web propose une méthode simple pour tous les utilisateurs d'une organisation d'accéder et de présenter le contenu.
- Application internet : les utilisateurs peuvent accéder à leurs courriers électroniques et créer des documents par exemple sans installer d'applications sur leurs ordinateurs.

Les organisations et les équipes peuvent aussi profiter de l'accès sécurisé aux applications d'entreprise via internet lors de leur déplacement et s'ils travaillent à distance.

- Application d'entreprise : les applications sectorielles d'entrepris doivent souvent déployer et gérer des installations coté client.
- Extranet : est un cas ou les utilisateurs extérieurs à l'organisation peuvent accéder à des données. La sécurité est un souci important, mais les applications Web représenter un bon choix parce qu'elles proposent une méthode standard grâce à laquelle les utilisateurs peuvent les utilisations peuvent accéder aux informations dont ils ont besoin.

Les services de rôle IIS

- Fonctionnalités http communes
- développement d'application
- Intégrité et diagnostics
- Service de publication FTP
- Outils de gestion

II.11.RADIUS

RADIUS (acronyme de Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des demandes d'authentification relayées par des équipements de réseau, comme des commutateurs ou bornes Wifi, considérés a Par extension, un serveur qui centralise des demandes d'authentification et les soumet à un service d'annuaire LDAP ou à un service de base de données SQL est appelé serveurRADIUS. Lors comme ses clients. [12]

RADIUS interroge une base de données d'authentification et d'autorisation qui peut être un domaine Active Directory, une base LDAP ou une base de données SQL.

Ces bases ou annuaires peuvent se trouver sur le serveur lui-même ou sur un serveur tiers. Certaines implémentations de RADIUS disposent d'une base de données en propre.

A l'origine, RADIUS était surtout utilisé pour l'identification des clients des FAI, ses capacités de comptabilisation des accès (accounting) permettant notamment la journalisation des accès et leur facturation. RADIUS a été utilisé par la suite en entreprise pour l'identification des clients finals WIFI et pour l'identification des clients finals câblés.

II.11.1.Rôles du serveur RADIUS

En premier lieu, RADIUS doit authentifier les requêtes qui sont issues des clients finals, via les clients RADIUS. Cette authentification se basera soit sur un couple identifiant/mot de passe, soit sur un certificat. Cela dépendra du protocole d'authentification négocié avec le client final.

En deuxième lieu, RADIUS a pour mission de décider quoi faire du client authentifié, et donc de lui délivrer une autorisation, un "laissez-passer". Pour ce faire, RADIUS envoie des informations (on parle "d'attributs") aux clients RADIUS. Un exemple typique d'attribut est un numéro du VLAN dans lequel placer le client authentifié etautorisé.

Enfin, en bon gestionnaire, RADIUS va noter plusieurs données liées à la connexion, comme la date et l'heure, l'adresse MAC de l'adaptateur réseau du client final, le numéro de VLAN...). C'est son rôle comptable ou "d'accounting".

RADIUS est donc un serveur d'authentification, d'autorisation et de comptabilité. De façon imagée, c'est le "chef d'orchestre" des connexions 802.1X et les clients RADIUS sont ses sbires... En ce sens, il se range dans le modèle AAA (Authentication, Authorization, Accounting).

NPS (Network Policy Server) est le nom du service RADIUS des systèmes Microsoft Windows 2008 Server, en remplacement du "Service d'Authentification Internet" de Windows 2003 Server. D'autres solutions propriétaires existent, comme CISCO ACS (Access Control Server). Différentes versions libres de RADIUS existent également, comme Free RADIUS (sous Linux ou Windows) ou Open RADIUS (sous Linux). RADIUS peut aussi servir à centraliser les accès sécurisés aux pages ou aux terminaux de paramétrage de tous les équipements réseau : commutateurs, routeurs, bornes wifi, contrôleurs wifi, etc.

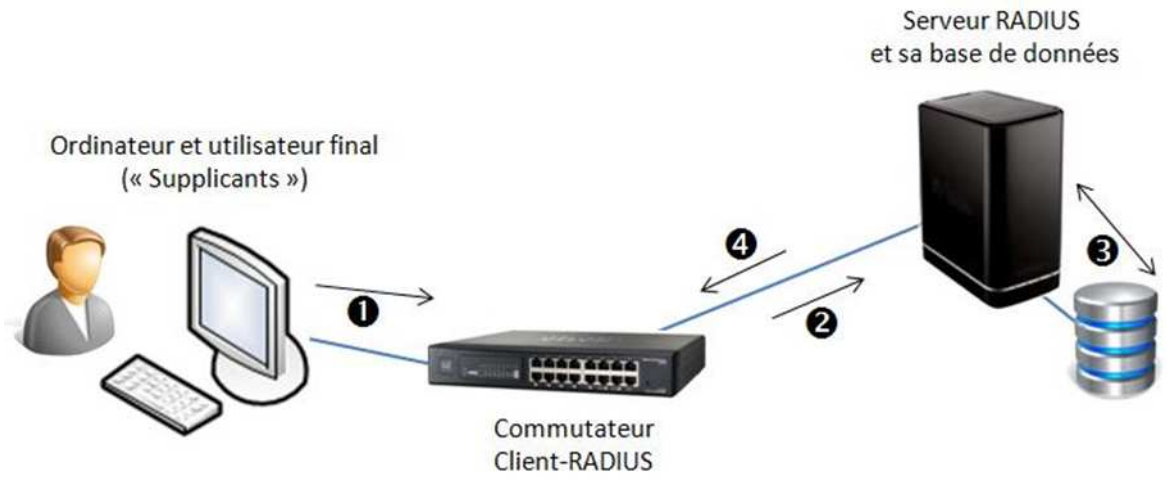


Figure II.9:Radiuse

II.12.La Zone Démilitarisée (DMZ)

II.12.1.Définition

Dans la sécurité informatique, une zone démilitarisée (DMZ) est un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre un réseau interne (LAN) et un réseau externe (internet). Sur ce réseau nous disposons d'un espace confiné, d'une taille limitée. Le nombre de serveurs présents sur ce réseau est limité, de sorte à ne pas permettre une trop grande interaction entre les serveurs. Dans ce réseau « haut sécurité », il n'y a aucun poste utilisateur, chaque flux à destination de l'une de ces serveurs (qu'il provienne d'internet ou d'un réseau interne) est clairement défini sur firewall. De cette manière, nous maitrisons précisément les connexions à destination et en provenance de ces machines.

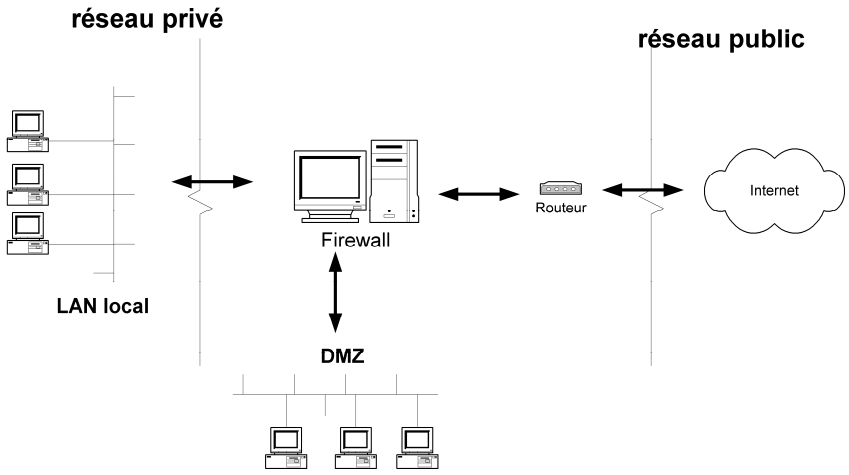


Figure II. 10:DMZ

II.12.2.Quelques règles spécifiques sont applicables aux DMZ

Il convient de sécuriser spécifiquement ces machines, en limitant les services rendu par ces serveurs. De plus, il faut désinstaller/désactiver ce qui ne serait pas nécessaire. Dans le cas d'un serveur Windows, il convient par exemple de désactiver le partage Windows.

Il ne faut surtout pas laisser trainer des exécutables de teste de réseau (type nmap.., etr.), surce serveur (même si ces dernier ne sont que des programmes d'installation). Si un hacher parvenait par un moyen non prévu à lance ces exécutables, il pourrait compromettre la sécurité de cette DMZ.

Les flux entre serveur au sien de la DMZ sont à la limiter. Si ces derniers sont nombreux et sensible, il faut dans ce cas envisager de mettre en place une second DMZ, déplacer certains de ces serveur sur la novelles DMZ et autoriser les flux spécifique sur le Firewall .Il est courant pour les architectures « avancées » de disposer d'un certain nombre de DMZ. Au final, il ne s'agit là que de segmenter les réseaux et de filtrer les interactions entre ces réseaux.

II.12.3. Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risque de compromettre la sécurité de l'entreprise.

Pour pouvoir applique la politique de sécurité de l'entreprise. Nous proposons de séparer les réseaux LAN de l'entreprise en mettant le serveur des fichiers et le serveur active directory dans la zone démilitarisé et les postes client dans une autre zone puis les interconnecter à l'aider des Switch et routeurs, pour gérer le trafic entre les zones nous allons implémenter ASACisco5510

La politique de sécurité mise en œuvre sur la DMZ est la suivante :

- Trafic du réseau externe vers la DMZ autorisée.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe autorisé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

II.13.PRÉSENTATION DE LA GAMME CISCO ASA 5500

La gamme Cisco ASA 5500 inclut les boîtiers de sécurité adaptatifs Cisco ASA 5505, 5510, 5520 et 5540.

Il s'agit de quatre serveurs desécurité ultra-performants issus de l'expertise de Cisco System® en matière de développement de solutions de sécurité et VPN reconnues et leaders sur leur marché. Cette gamme utilise les dernières technologies des serveurs de sécurité Cisco PIX® 500, des capteurs Cisco IPS 4200 et des concentrateurs Cisco VPN 3000.

Conçue comme l'élément principal de la solution Self-Defending Network de Cisco (réseau qui se défend tout seul), lagamme Cisco ASA 5500 permet de mettre enplace une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible.

Le résultat est une gamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux des PME/PMI et des grandes entreprises touten réduisant l'ensemble des frais de déploiement et d'exploitation et en simplifiant les tâches généralement associées à un tel niveau de sécurité.

II.14.Description des Serveurs de Sécurité Adaptatifs de la gamme Cisco ASA 5500

Les Serveurs de Sécurité Adaptatifs Cisco® ASA 5500 combinent les meilleurs services de VPN et de sécurité, et l'architecture évolutive AIM (Adaptive Identification and Mitigation), pour constituer une solution de sécurité spécifique.

Conçue comme l'élément principal de la solution Self-Defending Network de Cisco (le réseau qui se défend tout seul), la gamme Cisco ASA 5500 permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible.

Le résultat est une gamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux des PME/PMI et des grandes entreprises tout en réduisant l'ensemble des frais de déploiement et d'exploitation et ensimplifiant les tâches généralement associées à un tel niveau de sécurité.

Réunissant sur une même plate-forme une combinaison puissante de nombreuses technologies éprouvées, la gamme Cisco ASA 5500 vous donne les moyens opérationnels et économiques de déployer des services de sécurité complets vers un plus grand nombre de sites.

La gamme complète des services disponibles avec la famille Cisco ASA 5500 permet de répondre aux besoins spécifiques de chaquesite grâce à des éditions produits conçues pour les PME comme pour les grandes entreprises. Ces différentes éditions offrent une protection de qualité supérieure en apportant à chaque installation les services dont elle a besoin.

Chaque édition de la gamme Cisco ASA 5500 regroupe un ensemble spécialisé de services – firewall, VPN SSL et IPSec, protection contre les intrusions, services Anti-X, etc. – qui répondent exactement aux besoins des différents environnements du réseau d'entreprise.
Et lorsque les besoins de sécurité de chaque site sont correctement assurés, c'est l'ensemble de la sécurité du réseau qui en bénéficie.

II.15.Principaux avantages technologique et nouveautés de la gamme ASA 5500

La gamme Cisco ASA 5500 aide les entreprises à protéger plus efficacement leurs réseaux tout en garantissant une exceptionnelle protection de leurs investissements grâce notamment, aux éléments clés suivants :

- **Technologie reconnue de firewall et VPN protège contre les menaces**

Développée autour de la même technologie éprouvée qui a fait le succès du serveur de sécurité Cisco PIX et de la gamme des concentrateurs Cisco VPN 3000, la gamme Cisco ASA5500 est la première solution à proposer des services VPN-SSL (Secure Sockets Layer) et IP sec (IP Security) protèges par la premier technologie de firewall du marché.

Avec VPN-SSL, l'ASA 5500 est une passerelle SSL performante qui permet l'accès distant sécurisé au réseau au travers d'un navigateur web banalisé pour les utilisateurs nomades.

- **Service évolué de prévention des intrusions**

Les services proactifs de prévention des intrusions offrent toutes les fonctionnalités qui permettent de bloque un large éventuel de menaces –vers, attaques sur la couche applicative ou niveau du système d'exploitation, logiciel espions, messagerie instantanée.

- **Service anti-X à la pointe de l'industrie**

La gamme Cisco ASA 5500 offre des services complètes anti-Xà la pointe de la technologie-protection contre les virus, les logiciel espion, le courrier indésirable et le phishing ainsi que le blocage de fichier, le blocage et le filtrage des URL et le filtrage de contenu en associant le savoir-faire de Trend micro en matière de protection informatique à une solution Cisco de sécurité réseau éprouvée.

- **Service multifonctions de gestion et de surveillance**

Sur une même plate-forme, la gamme Cisco ASA 5500 forme des services de gestion et de surveillance utilisable de manier intuitive grâce au gestionnaire Cisco ASDM(Adaptative Security Device Manger) ainsi que des services de gestion de catégorie entreprise avec Cisco Security management suite.

- **Réduction des frais de déploiement et d'exploitation**

La solution multifonction CiscoASA5500 permet la normalisation de la plate-forme, de la configuration et de la gestion, contribuant à réduire les frais de déploiement et d'exploitation récurrents

II.16.Le fonctionnement d'ASA

L'ASA offre deux modes pour ces utilisateurs :Le mode routed » est de niveau 3 : quand il Ya de trafic, l'ASA est comme un saut sur routeur (routeur hop in the network).

Le mode » transparent » est de niveau 2 : il facilite la configuration du réseau et permet de cacher le pare-feu (aux intrus éventuels).on utiliser aussi le mode transparent pour autoriser le trafic qui est bloqué par un routeur en utilisent les ACLs0.

II.17.Les fonctionnalités d'ASA

II.17.1ACL (Access Control Lists)

A chaque interface connectée à l'ASA, niveau de sécurité (entre 0 et 100) est attribué, le niveau de sécurité 100 se voit attribué par défaut au réseau dont on a la maitrise (LAN) et le niveau 0se voit attribué au réseau extérieur .L'ASA interdit le trafic d'une interface vers une autre interface dont le niveau de sécuritéest élevé. Il autoriser le trafic d'une interface de niveau de sécurité est inférieur.

Les ACL (Access Listes) ont été mises en place pour pouvoir gérer le trafic entre les interfaces selon les besoin de l'entreprise.

II.17.2.Utilité d'une liste d'accès

Une liste d'accès vas servir à :

- A supprimer des paquets pour des raisons de sécurité.
- A filtrer des mises à jour de routage.
- A filtres des paquets en fonction de leur priorité(QOS : Quality of Servise)
- A définir du trafic intéressant pour des configurations spécifique (NAT, ISDM,….etc.)

II.17.3.Principe de fonctionnement

Une liste d'accès, comportant une suit d'instructions de filtrage, va être applique sur une interface du routeur, pour le trafic sortant. Il va falloir applique une logique sur les interfaces en sortie ou en entrée

- Les paquets peuvent être filtres en entrée (quand ils entrent su une interface avant la décision de routage.
- Les paquets peuvent être filtrés en sortie (avant de quitter une interface) avant la décision de routage.
- Le mot clef IOS est « deny » pour signifie que les paquets doivent être filtrés, précisément les paquets seront permis selon les critères définis.
- La logique de filtrage est configurée dans les listes d'accès.
- Une instruction implicite rejette tout le trafic à la fin de chaque liste d'accès.

II.17.4.Type d'ACL

Il existe deux types d'ACL :

- **ACL Standard :** Permet d'analyser du trafic en fonction de l'adresse IP source, elles sont appliquées le plus proche possible de la destination en raison de leur faible précision.
- **ACL Etendues** : Permet d'analyser du trafic en fonction d'adresse IP source, adresse IP destination, port source, port destination et protocole (IP, TCP, UDP, ICMP…), elles sont appliquées le plus proche possible de la source.

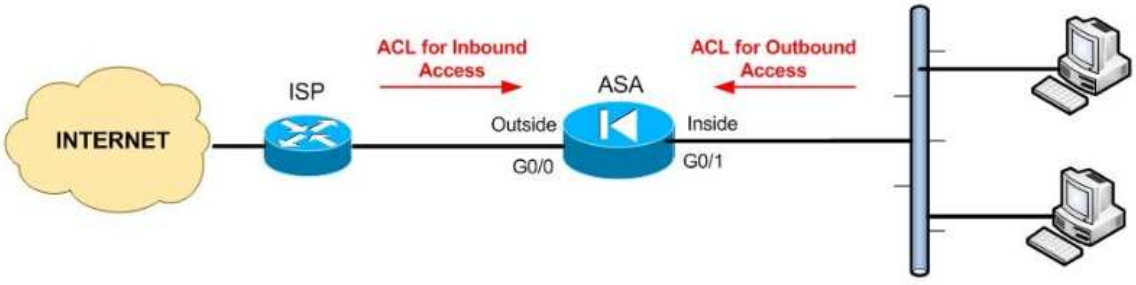


Figure II. 11:ACL

II.18.Translation d’adresse (NAT)

II.18.1.Principe du NAT :

Le mécanisme de translation d'adresses (en anglais Network Address Translation noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (leprotocole IPv6 répondra à terme à ce problème).
En effet, en adressage IPv4 le nombre d'adresses IProutables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines le nécessitant d'être connectées àinternet.

Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau. [13]

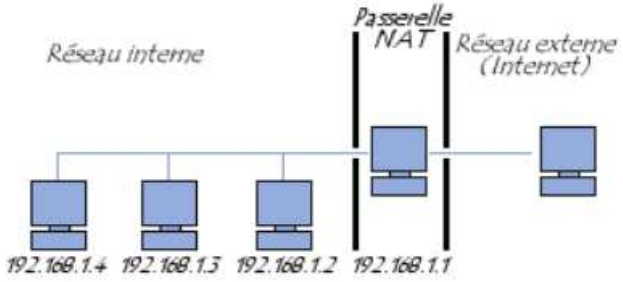


Figure II. 12:passerelle NAT

Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction») des paquets provenant du réseau interne vers le réseau externe.
Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, lapasserelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande.

Étant donné que la passerelle camoufle complètementl'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de sécurisation.En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.

On distingue deux types du NAT :

- **NAT statique** : elle consiste à associer à une adresse IP interne une adresse IP externe La correspondance est fixe.
- **NAT dynamique :** une plage d’adresse publique est mise au niveau du routeur et lorsqu’ une machine du réseau local veut accéder à internet, on lui attribue temporairement et dynamiquement une adresse publique prise dans cette plage.

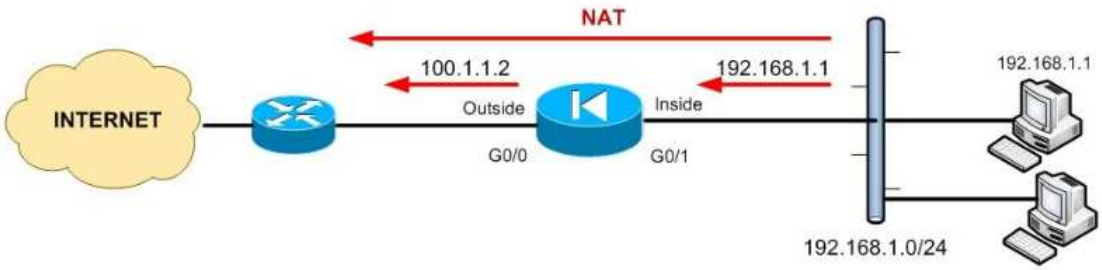


Figure II. 14:NAT

II.19.PAT (Port Address Translation) ou Overloading

Principe

Le port Addres Translation vient complémenter le NAT. En effet, supposant que nous ne disposons pas d'adresse IP publique suffisantes pour toutes nos machines locales, il va donc falloir partager réutiliser nos adresses.

PAT permet à plusieurs hôtes internes de partage adresse unique sur une interface externe en ajoutant des numéros de port différent à chaque connexion c'est-à-dire que Pour distingue les requêtes des différentes machines, on va utiliser le numéro du port.

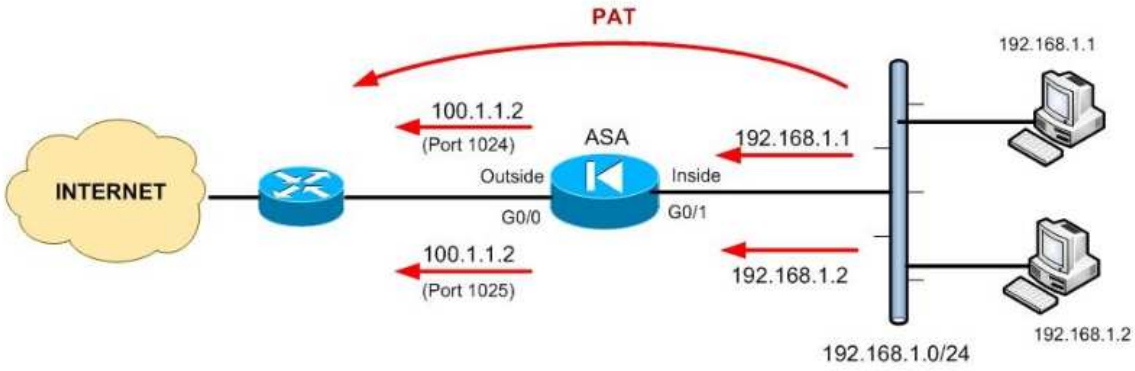


Figure II.15:PAT

II.20.Serveur de sécurité adaptatif Cisco ASA5510

Le serveur de sécurité adaptatif Cisco ASA 5510 propose des services évolués de réseau et de sécurité aux petites et moyennes entreprises et aux filiales et agences des grandes entreprises, sous la forme d'une solution économique et facile à déployer.

II.20.1.Les avantages d'ASA Cisco 5510

La gamme Cisco ASA 5510 fournit des services de pare-feu et de VPN ultraperformants, des services de prévention des intrusions et de réduction des vers

extrêmement sophistiqués grâce au module AIP SSM ou des services complets de protection contre les programmes malveillants grâce au module CSC SSM.

Les entreprise peuvent déployer jusqu'à cinq pare-feu virtuels dans une même Appliance afin de compartimenter le contrôle des politiques de sécurité au niveau des services

Cette virtualisation renforce la sécurité et réduit les couts globaux de gestion et d'assistance tout en permettant le regroupement de plusieurs périphériques de sécurité dans une même Appliance

II.21.Discussion

Dans ce chapitre nous avons présente le réseau d'une entreprise existant ainsi ses critique, après avoir examinées failles, la solution proposée était de réorganiser l'architecteurs du réseau et de centraliser leurs base de données. Ce que nous pouvons affirmer après notre étude, c'est qu'il faut mettre à jour l'infrastructure réseau (réseau et systèmes) avec des moyens récents et effectuer des test en tenant comptes des nouvelles technique de piratages pour optimiser les chances de sécurités.

Dans le chapitre suivant nous allons présenter les différentes étapes qui nous permettront la bonne réalisation de notre application.

Chapitre 2 RRRRRRRRRRRRRRR

III.1.Préambule

Quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité, il reste difficile, voire impossible, d'assurer la sécurité à 100%. L'avènement d'internet et des nouvelles technologies donnent une raison et une curiosité motivante aux pirates et aux malveillants de pénétrer de plus en plus dans les réseaux que ce soit par fun ou pour usurper des données et informations confidentielles.

Dans cette solution nous essaierons de minimiser au maximum les risques d'attaques et les points vulnérables de l'entreprise en accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

Dans ce chapitre, nous présenterons les différentes étapes suivies afin d'implémenter les solutions citées précédemment.

III.2.les étapes suivies pour la mise en place de notre application

Vu qu'il est impossible d'implémenter toute l'infrastructure réseau de l'entreprise avec les solutions réseaux et systèmes proposées. Nous avons simplifié l'architecture de sorte à permettre la mise en place de notre politique de sécurité. La figure suivant montre l'architecture simplifiée

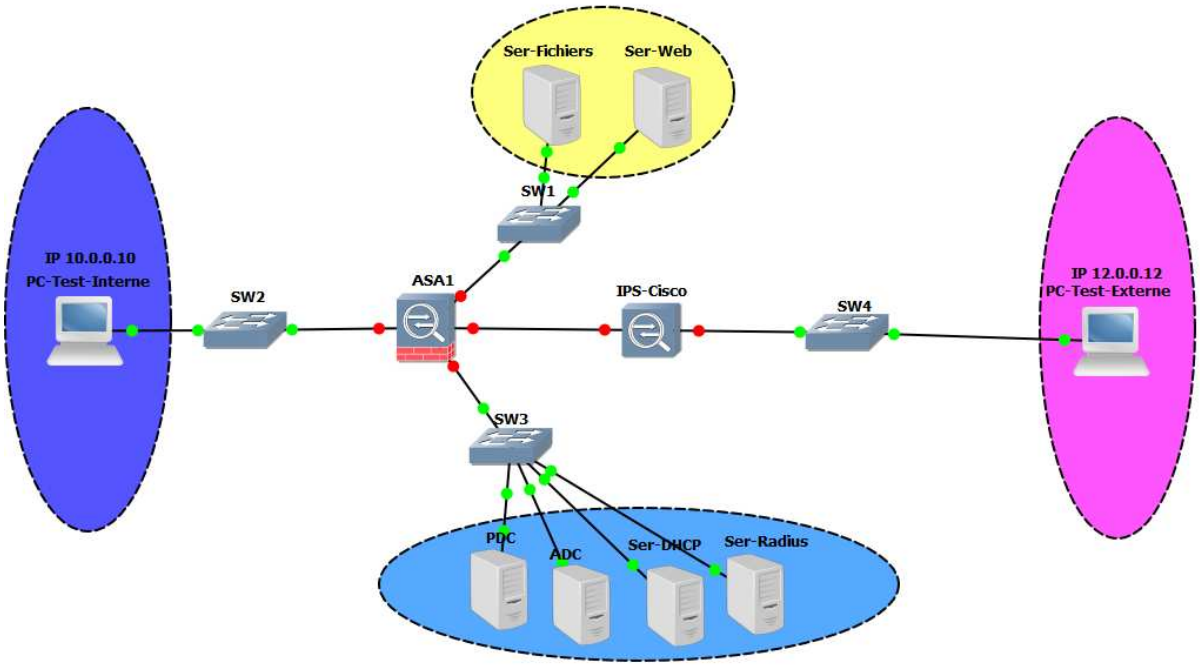


Figure III. 1: Infrastructure réseau mise en place sous GNS3.

Dans ce qui suit, nous présentons les différentes étapes suivies pour la réalisation de notre application.

III.2.1.Etape I : la préparation des machines

Nous avons préparé les machines suivantes :

Un contrôleur de domaine principal.

Un contrôleur de domaine secondaire.

Un serveur membre pour l'installation de serveur Web.

Un serveur membre pour l'installation de serveur Radius.

Un serveur membre pour l'installation de serveur DHCP.

Une machine membre client interne qui fait office de machine test.

Une machine (internet) client externe qui fait office de machine test.

a. L'installation du contrôleur de domaine principal et secondaire

Après préparation de deux machines virtuelles Windows Server 2012, nous avons installé sur la première machine un contrôleur de domaine principal (PDC), **2intparteners.com.** Sur la deuxième machine nous avons effectué le déploiement du contrôleur de domaine pour avoir un contrôleur de domaine secondaire (ADC). Ce dernier sert à la réplication du PDC. L'installation des deux contrôleurs est la même à la différence du choix de l'étape montrée ci-dessous. La première figure montre le choix de la création d'un nouveau domaine principal et la deuxième l'installation d'un contrôleur de domaine secondaire.

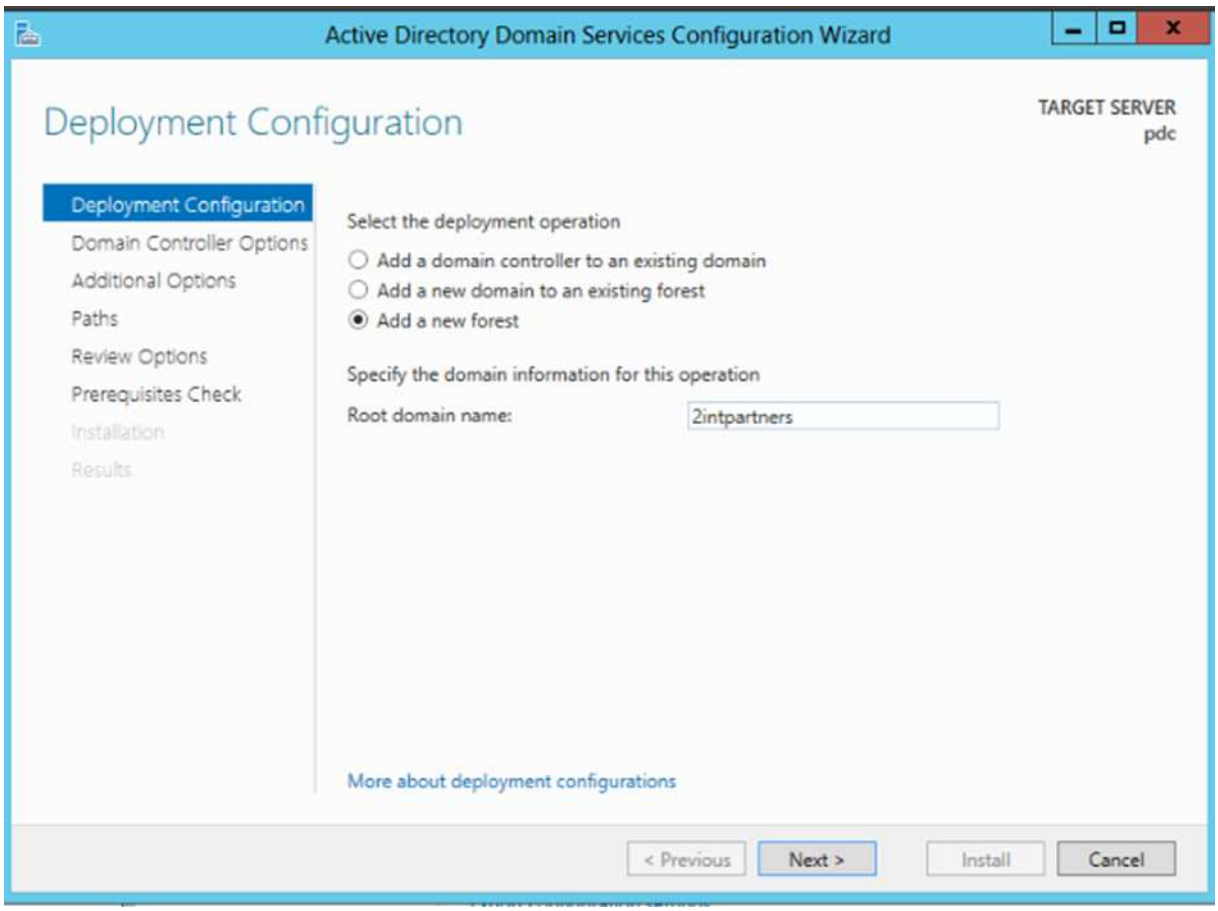


Figure III. 2 : La création du domaine principal.

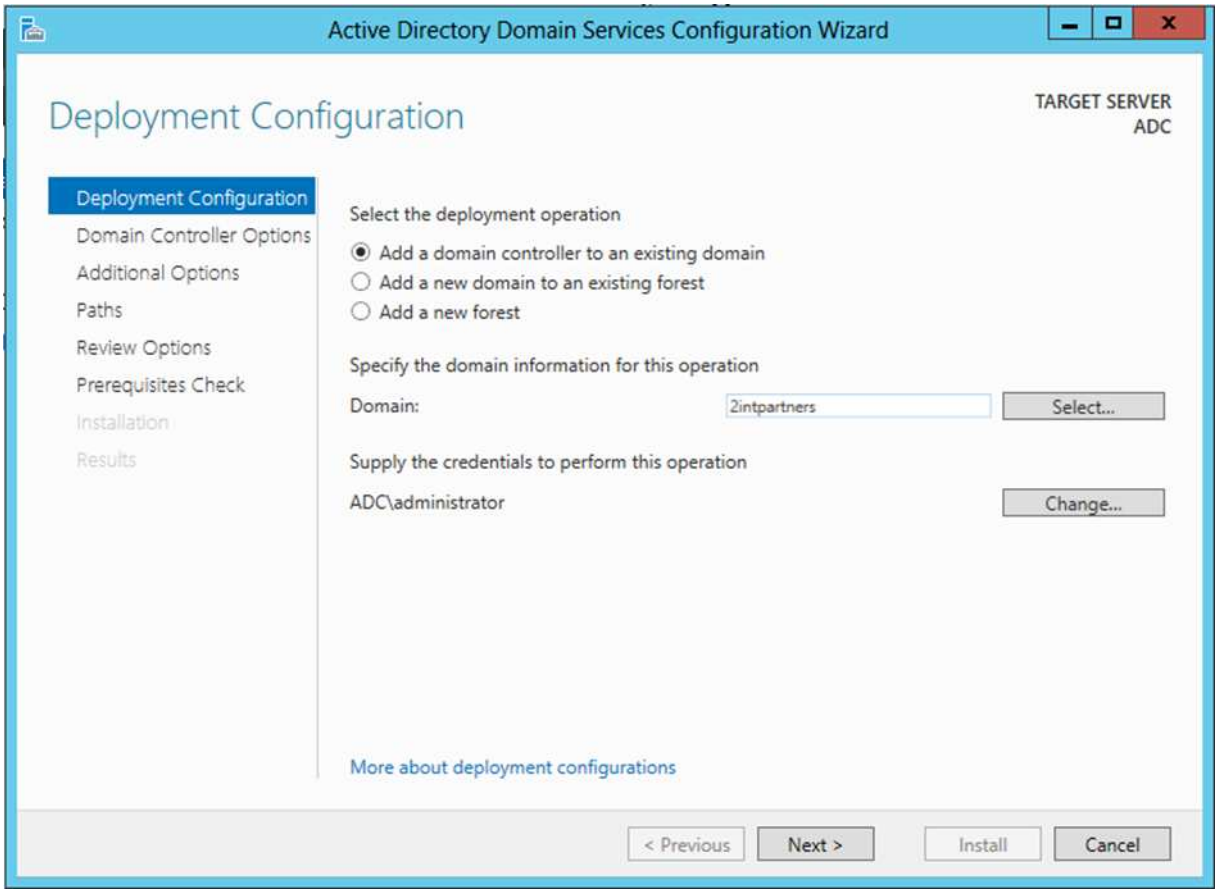


Figure III. 3: L'ajout du domaine secondaire.

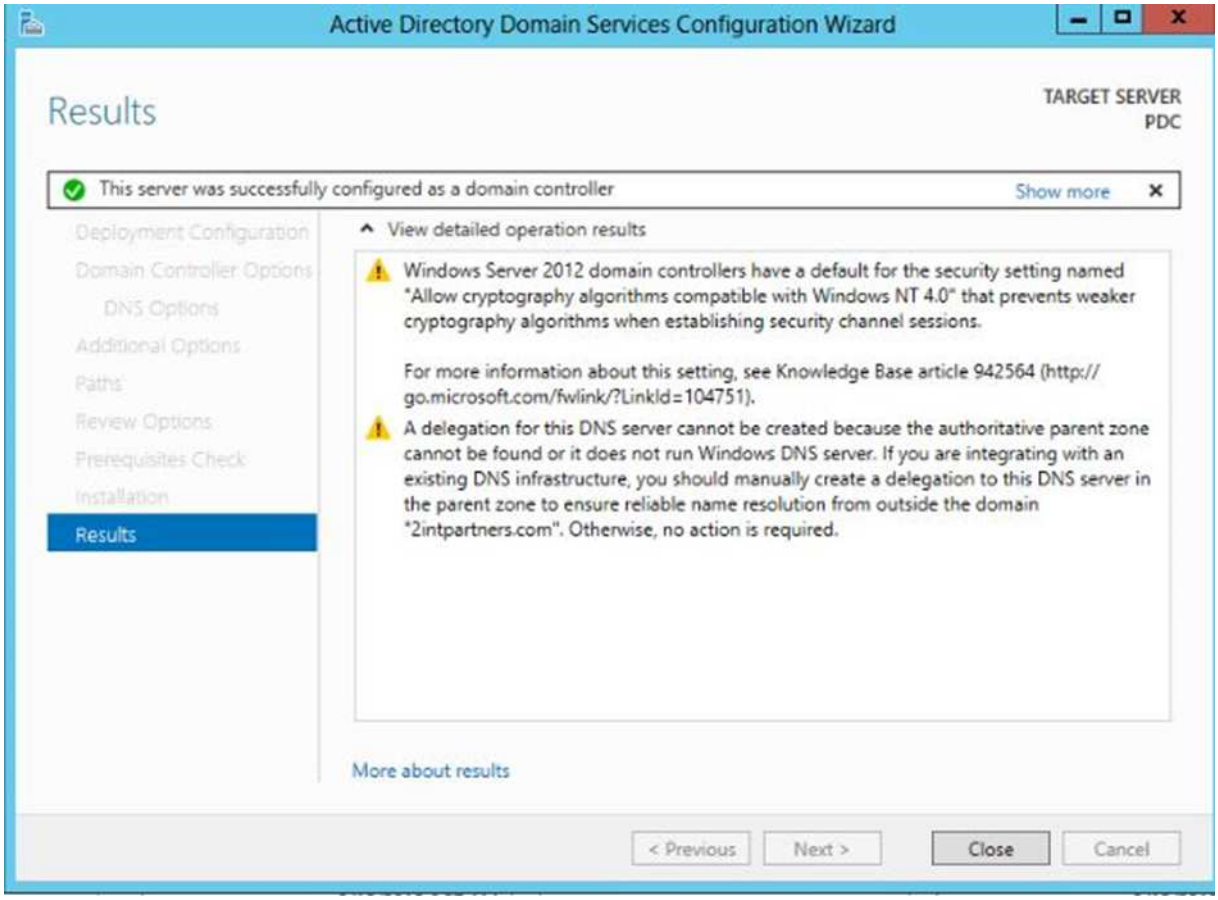


Figure III.4.résultat obtenu

b L'ajout d'un serveur ou machine membre

Un serveur ou une machine membre ne sont pas des contrôleurs de domaine mais seulement des membres du domaine. Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure suivante :

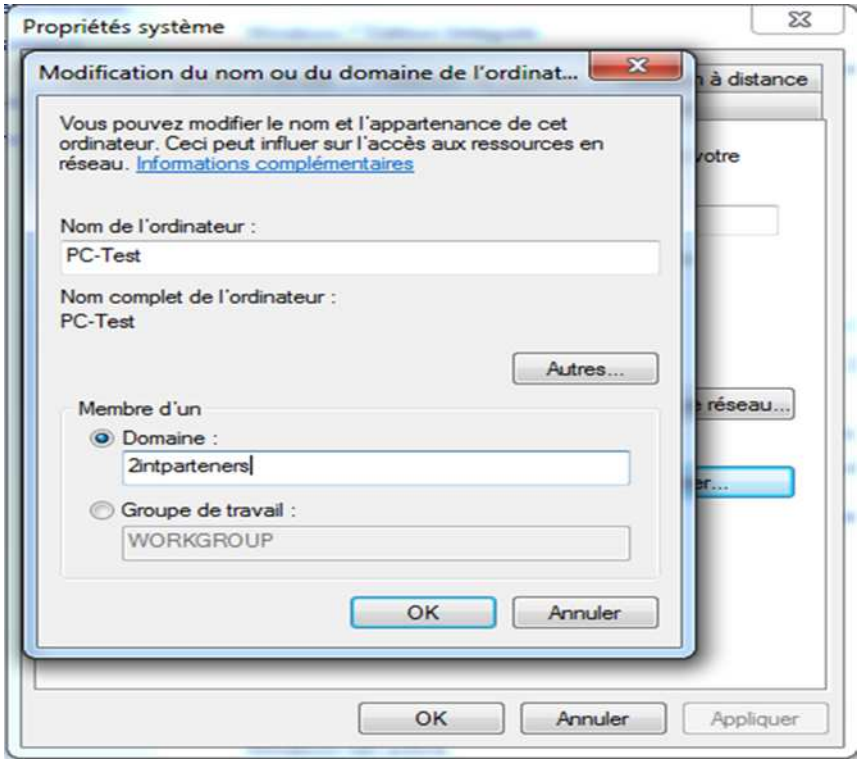


Figure III. 4: Ajout de la machine PC-Test au Domaine 2intparteners.com

III.2.2.Etape II :

a. Installation du serveur Web

L'installation du serveur Web consiste à installer le rôle « serveur web (IIS) » comme le montre la figure suivante :

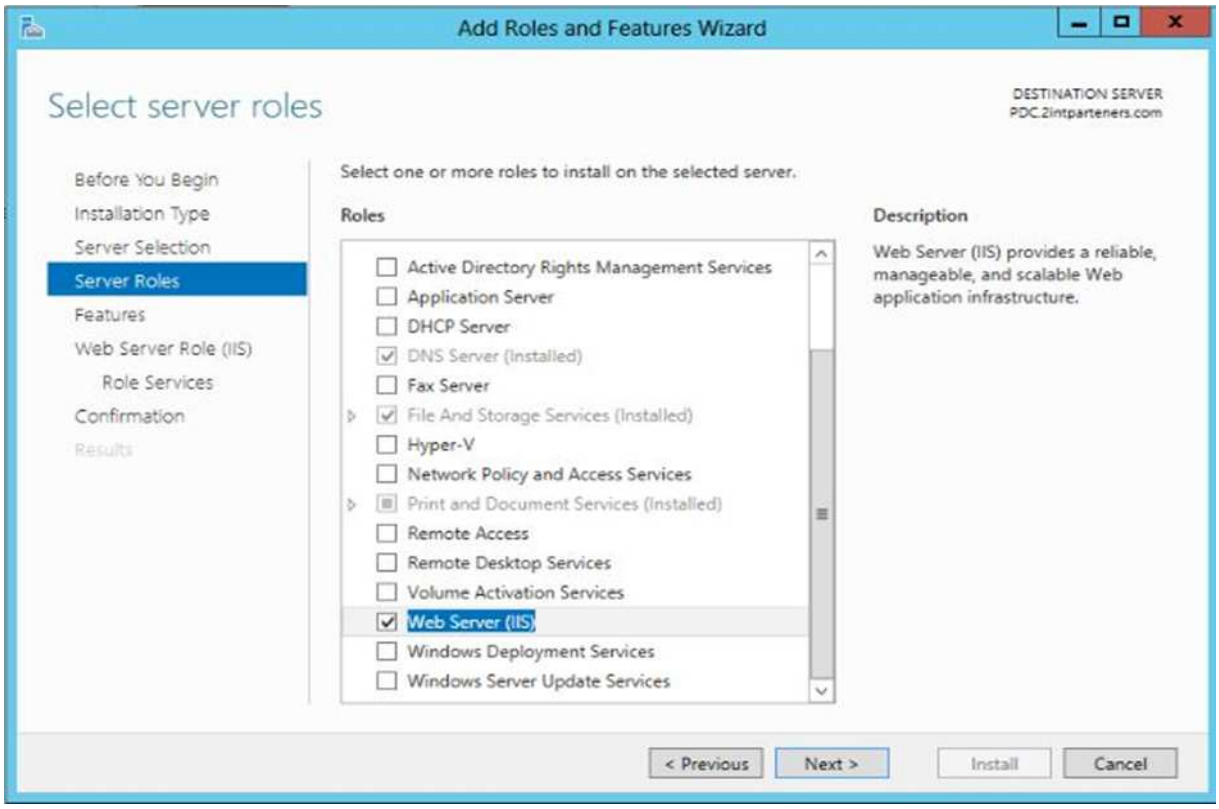


Figure III. 5 : L'installation du serveur web

Apres l'installation du service IIS on va créer un site web :

Dans le menu démarrer , outils d'administration, la fenêtre de dialogue suivante s'ouvre et on clique sur « Ajouter un site web ».

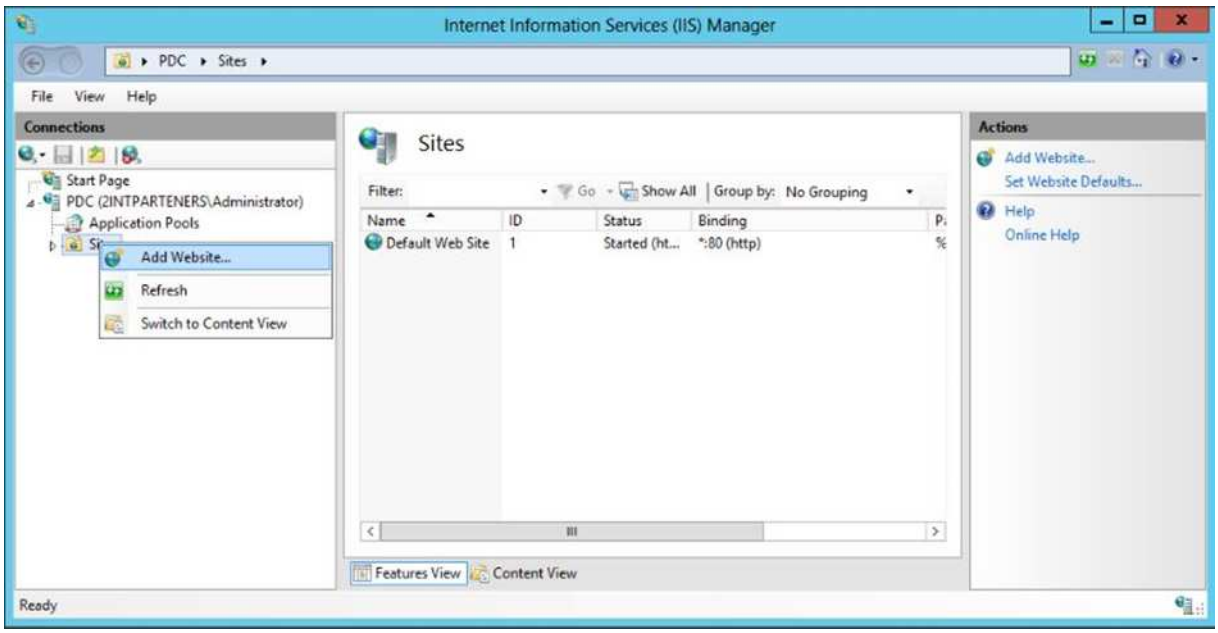
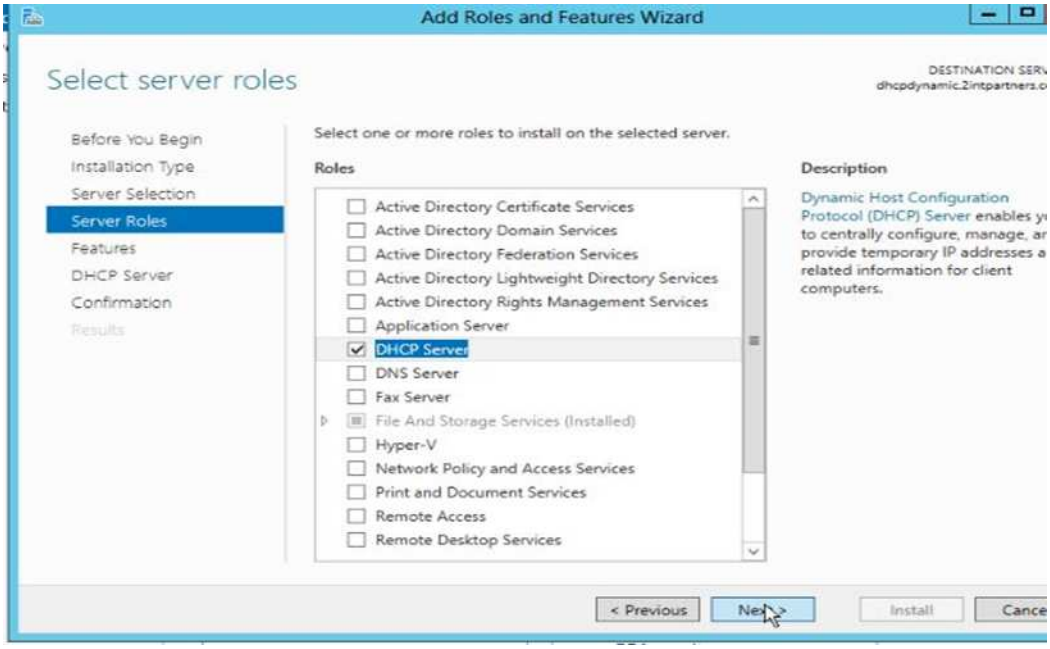


Figure III. 6 : Ajout d'un site web.

b. Installation du serveur DHCP

c.L'ajout de rôles serveur DHCP

Ayant affecté au PDC une adresse IP statique compatible avec la plage d'adresse prévue pour le sous-réseau local (12.0.0.0/8), lançons l'assistant Ajout de rôles depuis le Gestionnaire de serveur.



➢

Figure III. 7 : Ajout du rôle DHCP.

Sélectionnons l'adresse IP affectée manuellement, ce qui sera le sous-réseau logique des adresses qui seront affectées aux clients.

Figure III. 8: Sélection des liaisons de connexion réseau.

La spécification des paramètres du serveur WINS IPv4 permet de configurer l'option WINS, grâce à laquelle nous pouvons affecter une liste de serveurs WINS aux clients. Dans notre cas n'ayant pas de serveur WINS, cette option n'a pas été validée.

L'ajout d'étendues DHCP permet de définir ou de modifier les étendues sur le serveur DHCP. Notre étendue d'adresses IP pour les ordinateurs du sous-réseau DHCP est 10.0.0.100-120/8.

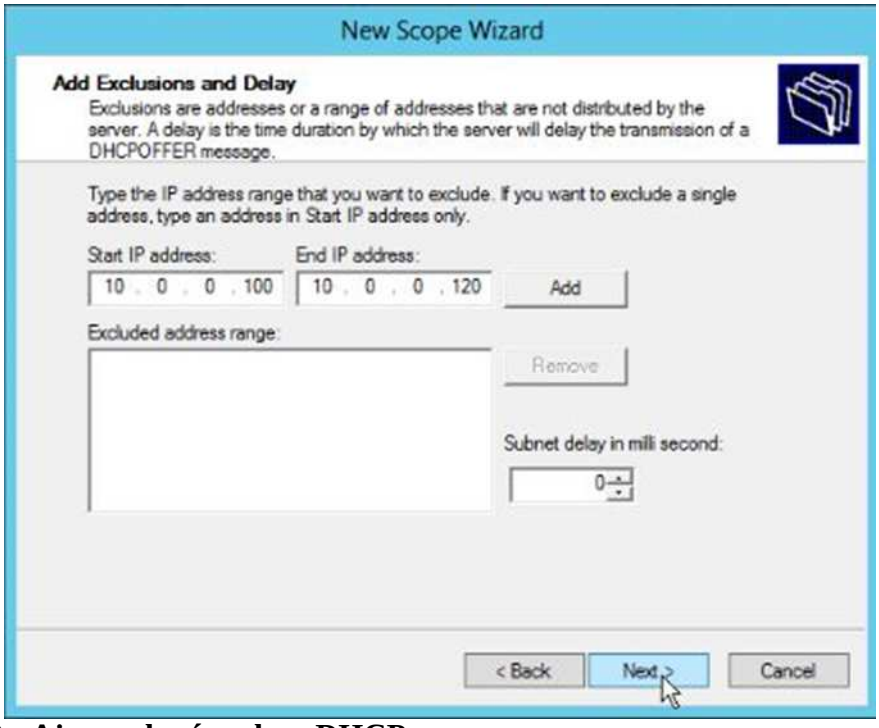


Figure III. 9 : Ajouter les étendues DHCP.

Pour sécuriser les échanges au niveau interne et limiter les accès depuis l'extérieur aux personnes autorisés pour la connexion au Switch. Nous allons dans ce qui suit installer un serveur Radius avec l'option 802.1x (NPS).

d. Installation du NPS (serveur Radius avec l'option 802.1x)

Pour installer le rôle NPS, nous suivons les étapes que voici:

Gestionnaire de serveur -> Ajouter des rôles ->Network Policy and Access Services.

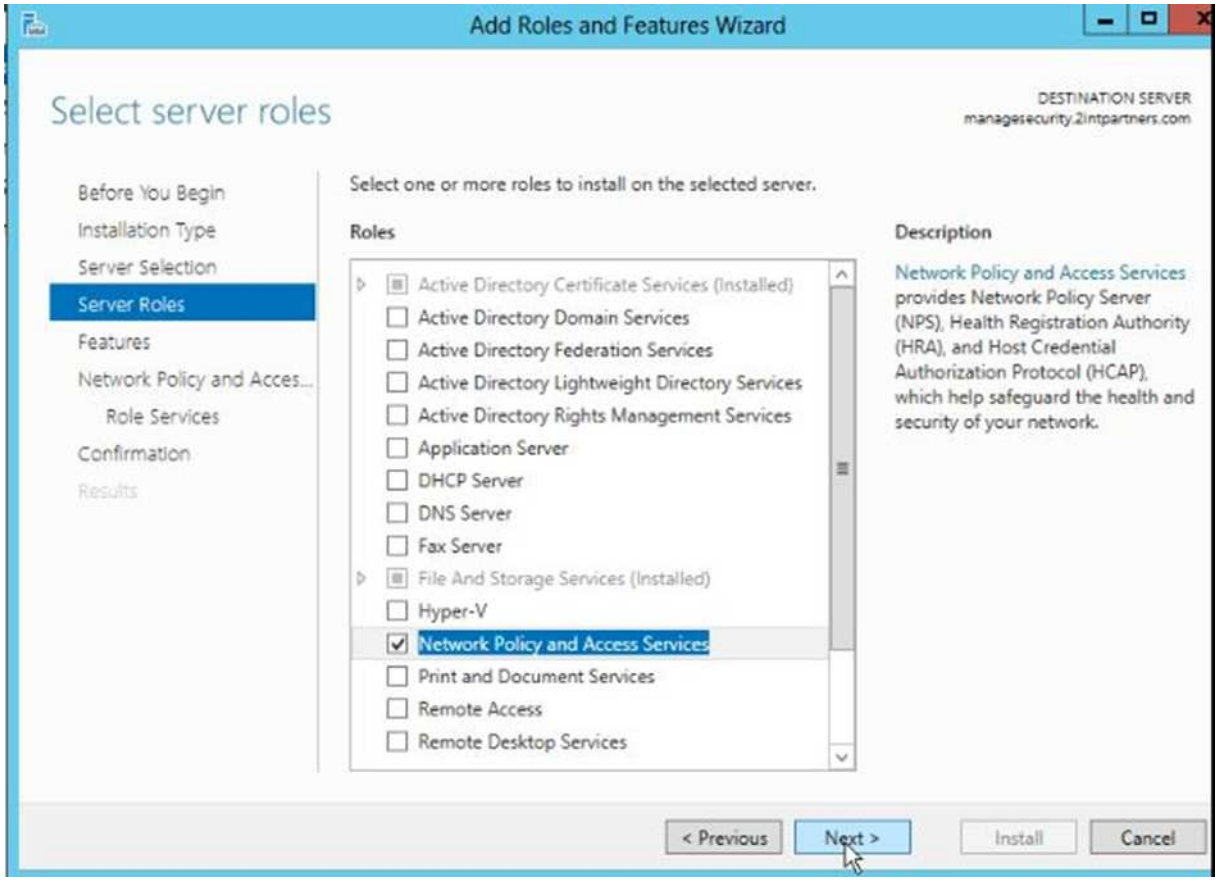


Figure III. 10 : Ajout du rôle Network Policy and Access Services.

Après la confirmation nous allons sélectionner l'option 802.1x avec une connexion Ethernet.

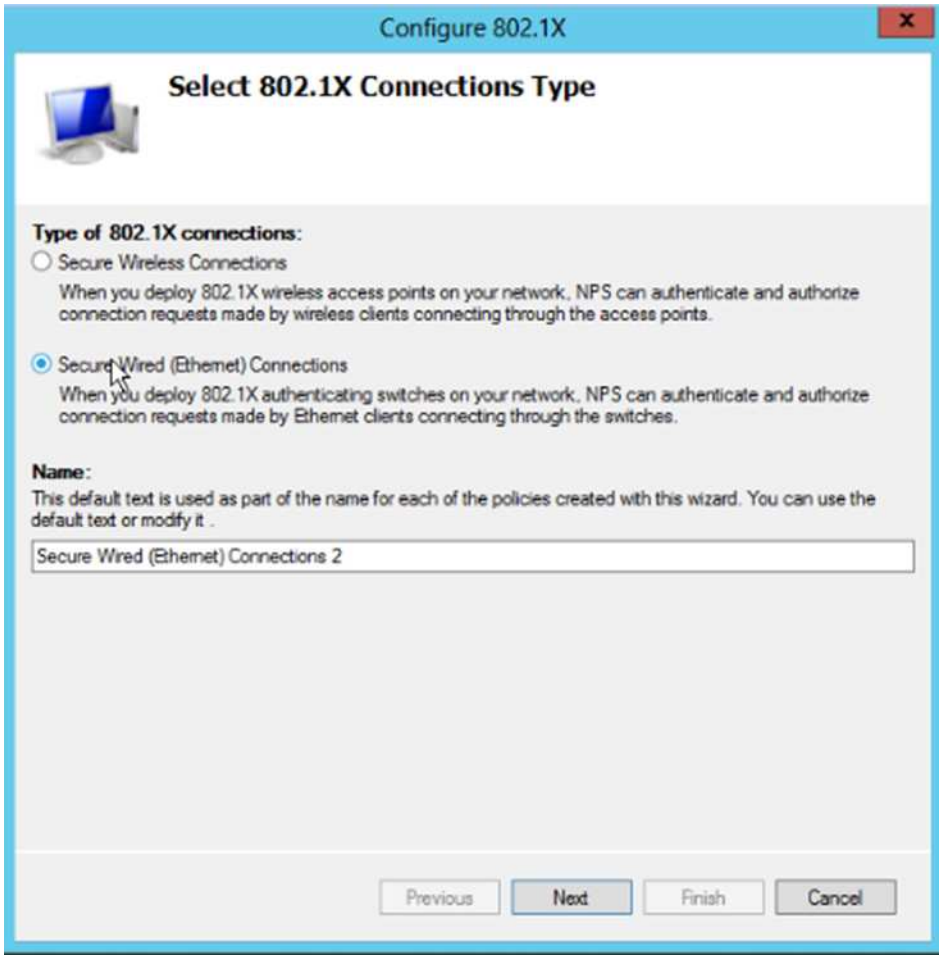


Figure III. 11 : Sélection d'une connexion Ethernet.

Ensuite nous allons introduire l'adresse IP du switch et saisir un mot de passe avec une configuration manuelle.

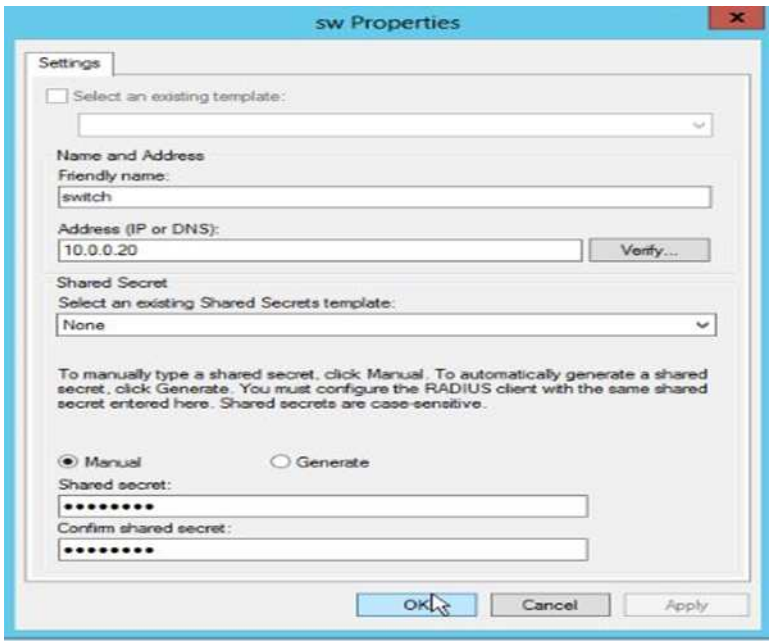


Figure III. 12 : Propriétés du Switch

Ensuite nous allons spécifier le groupe d'utilisateurs (**2INTPARTENERS/NPS-aaa**) en l'ajoutant, si vous n'avez pas encore créé un groupe vous pouvez le créer.

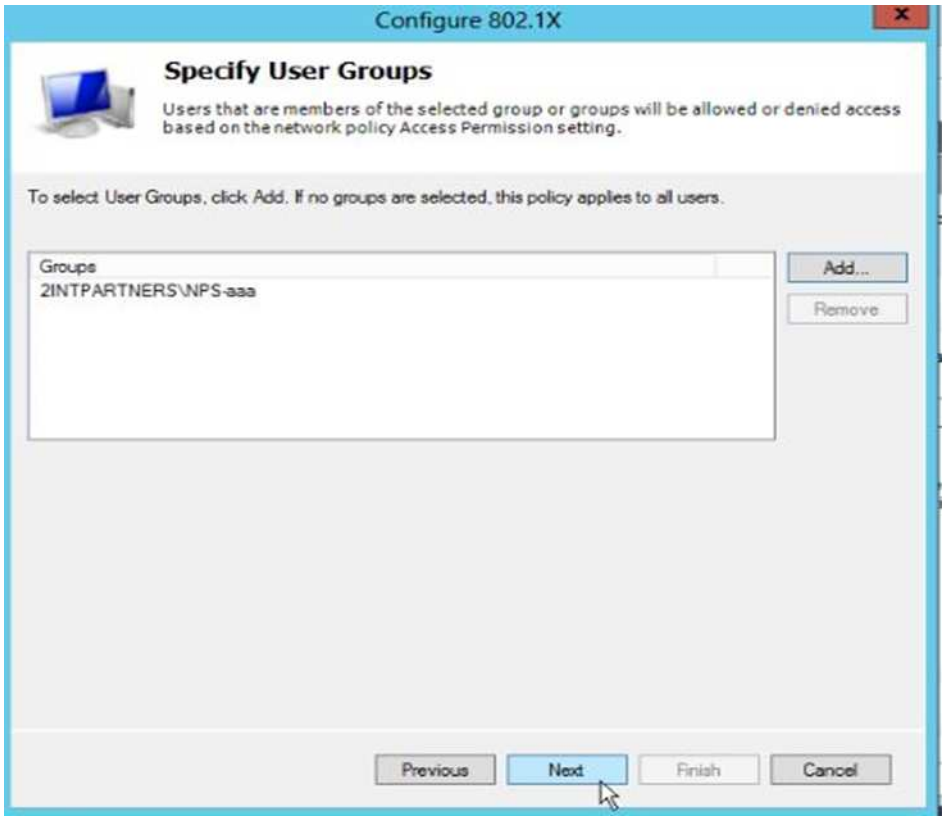


Figure III. 13 : Ajout du groupe d'utilisateurs.

En cliquant sur suivant une fenêtre nous résume l'installation comme étant créé avec succès.

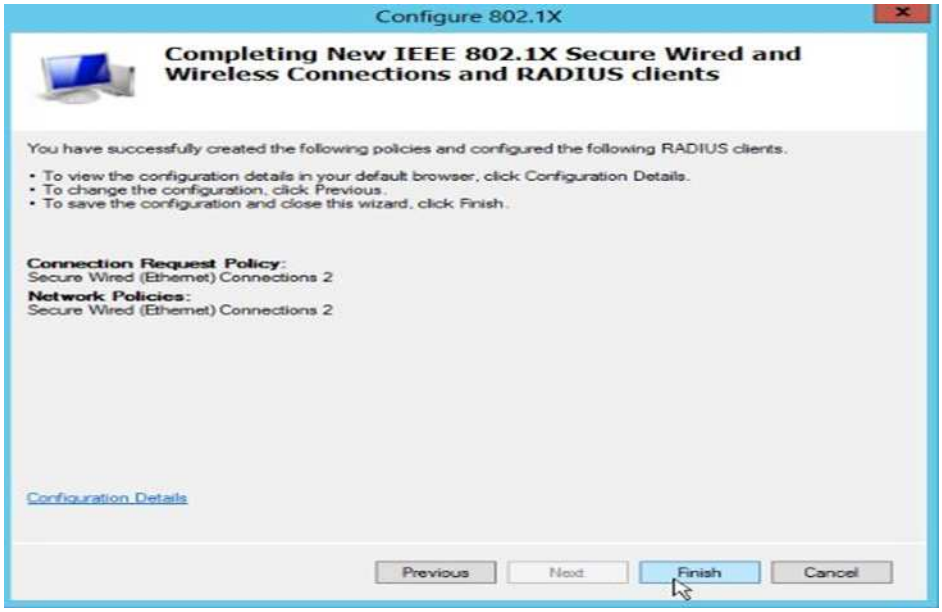


Figure III. 14 : Client Radius crée avec succès.

e. Installation de l'Autorité de Certification

Pour installer le service de certificats Active Directory, nous suivons les étapes que voici: Gestionnaire de serveur -> Ajouter des rôles -> Service de certificats Active Directory.

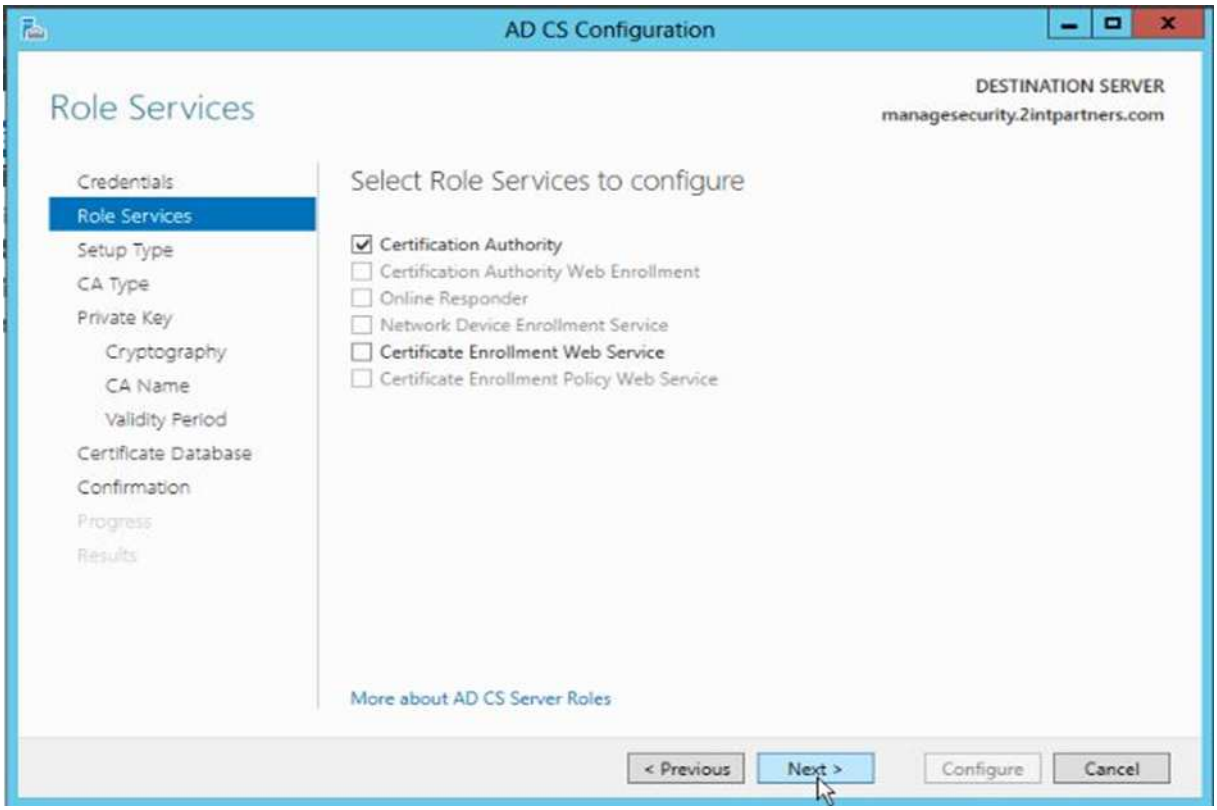


Figure III. 15 : Ajout du service de certificats Active Directory.

Ajout des rôles autorité de certification (CA) pour émettre et gérer les certificats et l'inscription web qui permet aux utilisateurs de se connecter à la CA via un navigateur web pour demander des certificats.

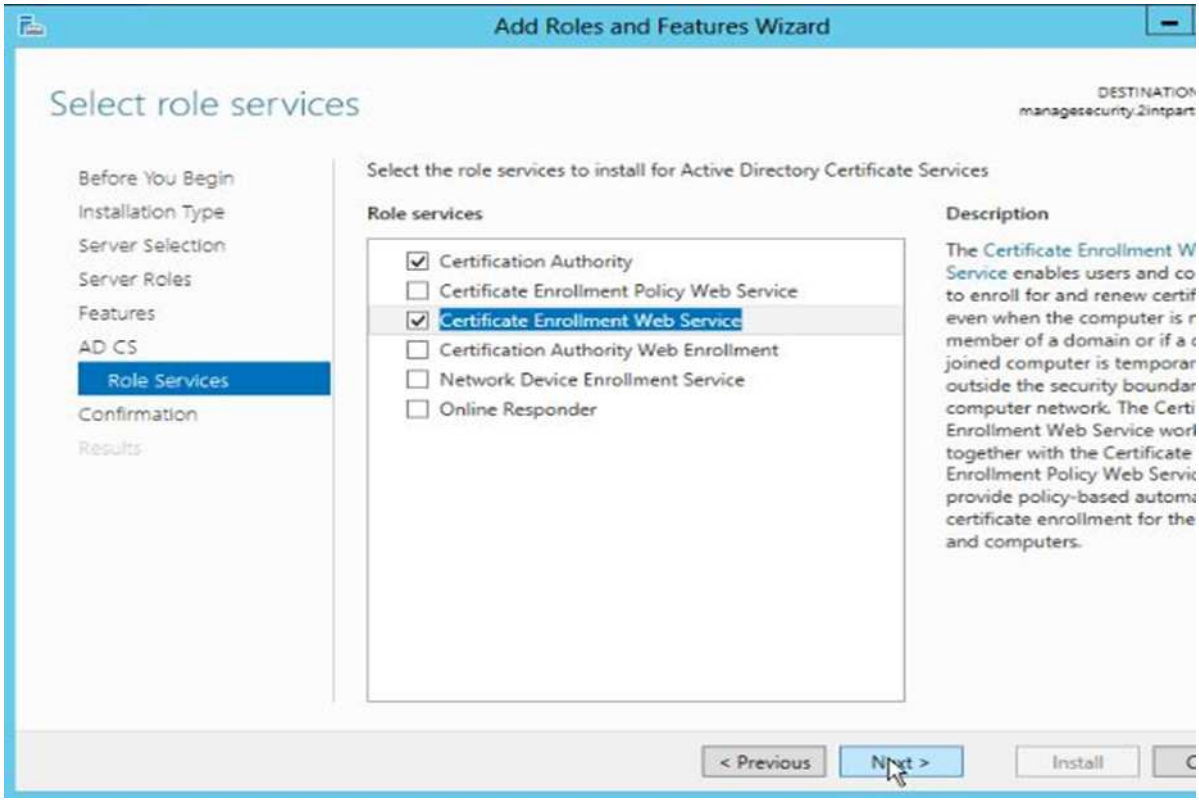


Figure III.16: Les services de rôle.

Lors de l'installation, il faut spécifier le type de l'installation de la CA, Autonome ou Entreprise. Autonome signifie que la CA n'est pas nécessairement intégrée dans un service d'annuaire AD alors que l'entreprise exige d'avoir un service annuaire. Notre choix s'est porté sur Entreprise cette CA qui sera utilisée comme émettrice. Elle sera subordonnée à une autre CA dans une hiérarchie, fournissant de ce fait des certificats aux utilisateurs autorisés, intérieurs et extérieurs.

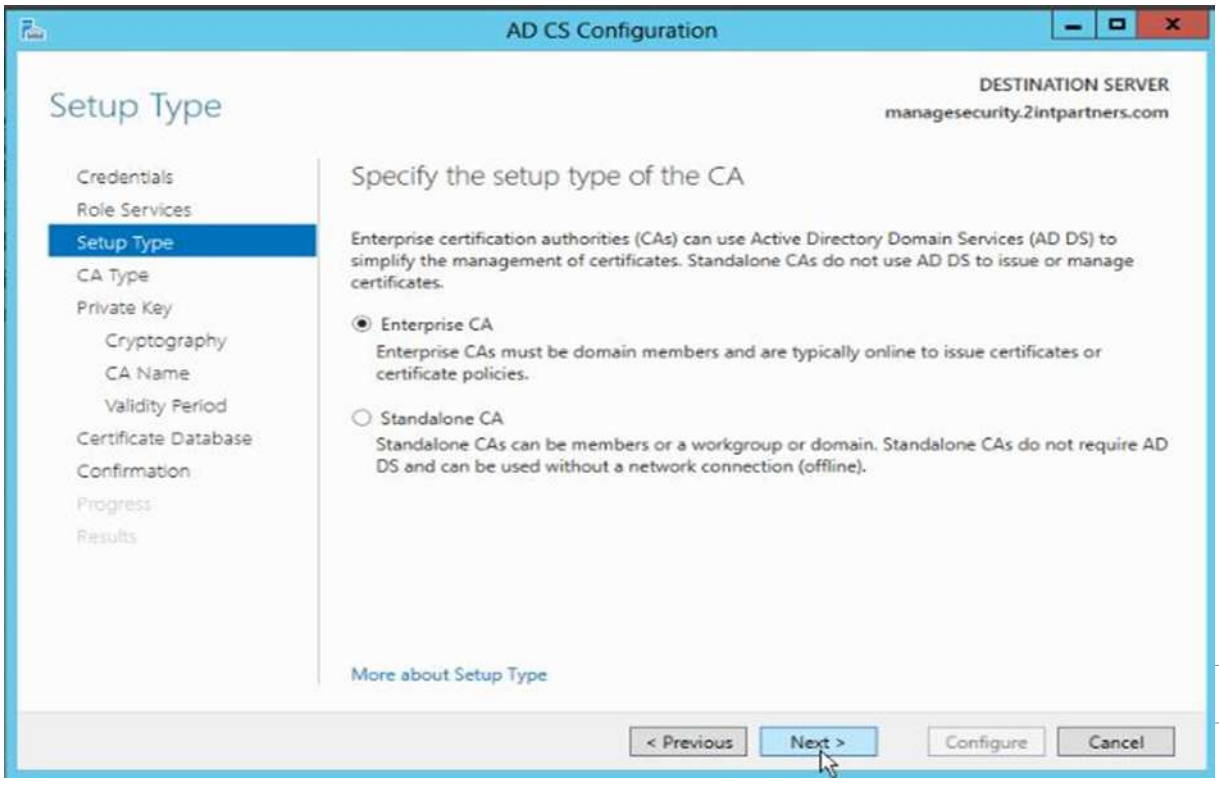


Figure III.17: Spécification du type d'installation.

Figure III.18: Création d'une nouvelle clé privée.

Définissons le nom de l'autorité de certificat, **root2intparteners-CA**

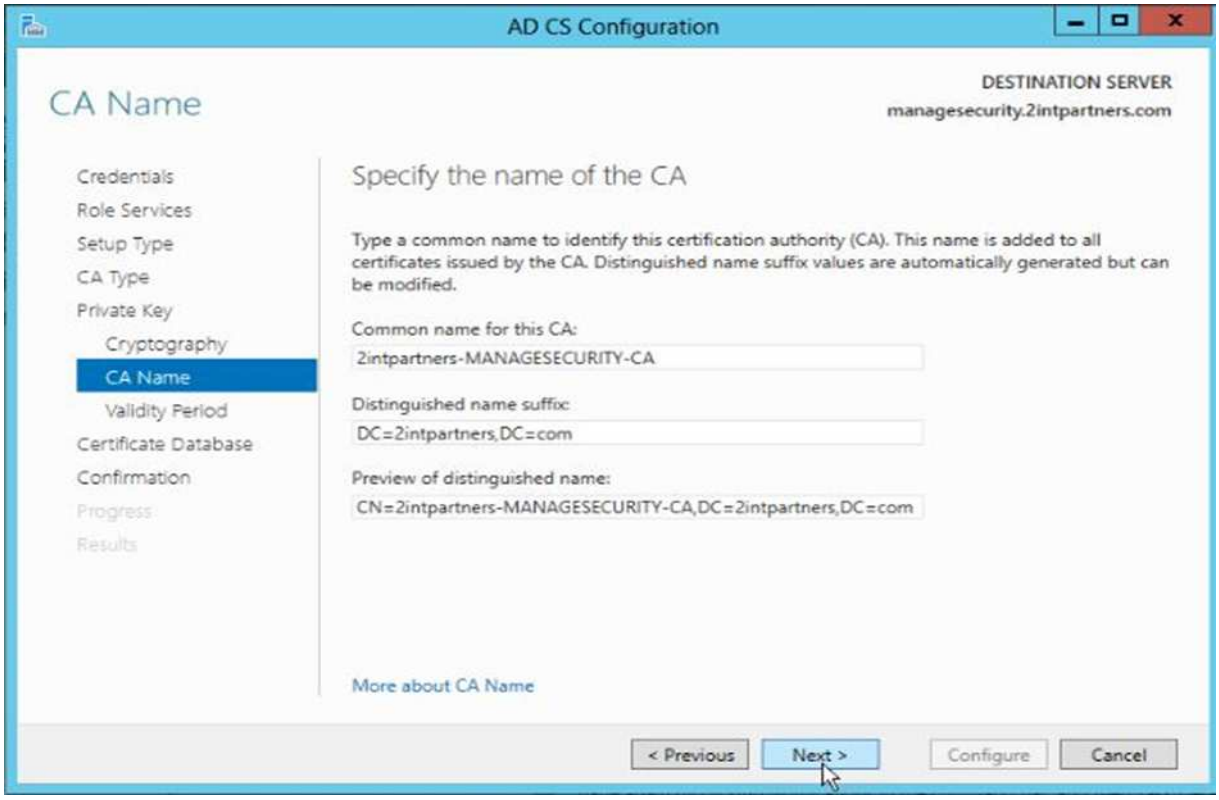


Figure III. 19: Nomination de l'Autorité de certificat

Pour le choix de la méthode d'authentification crypté nous avons choisi le (MS-CHAP-v2) avec la possibilité de changement de mots de passe.

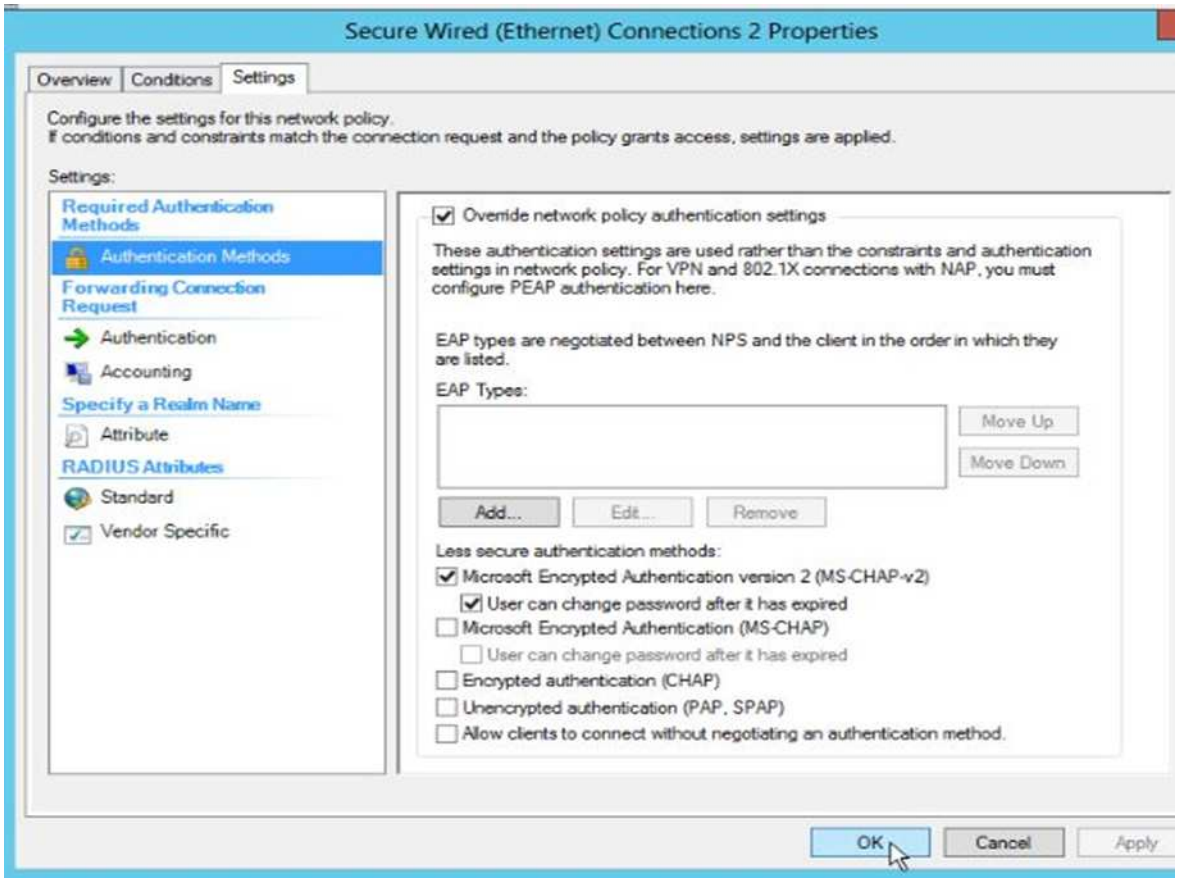


Figure III.20 : le choix de la méthode d'authentification (MS-CHAP-v2).

A la fin, le résultat obtenu une configuration avec succès.

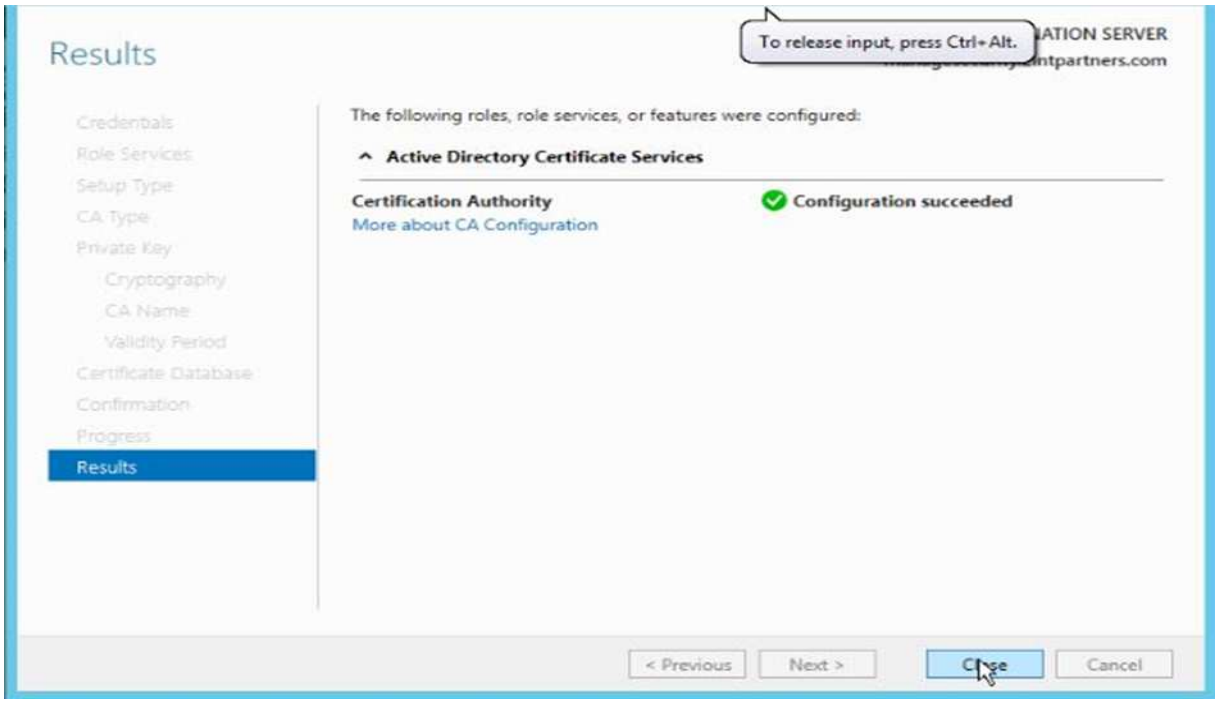


Figure III.21 : configuration avec succès.

III.2.3.Etape 3 : Installation et déploiement de Kaspersky Administration Kit 8

Nous installons Kaspersky administration kit 8 sur le contrôleur de domaine principal PDC et nous le déployons sur l'ensemble de la forêt**2intparteners.com.**

a. Déploiement de Kaspersky Administration Kit

Il existe plusieurs options de déploiement et de protection antivirus administrés par Kaspersky sur les ordinateurs du système réseau qui sont :

b. Installation à distance centralisée des applications sur les postes clients :

Dans ce cas, l'installation des applications et la connexion au système d'administration à distance centralisé s'opère automatiquement, ne demande aucune intervention de l'administrateur et permet d'installer le logiciel antivirus sur n'importe quel nombre de postes clients.

c. Installation locale des applications sur chaque poste client :

Dans ce cas, l'installation des composants requis sur les postes clients et sur le poste administrateur s'opère manuellement. Les paramètres de connexion des clients au serveur seront définis lors de l'installation de l'Agent d'administration. Cette option de déploiement est utilisée dans le cas où il n'est pas possible d'exécuter une installation à distance centralisée.

Afin de faciliter le déploiement de l'anti-virus sur l'ensemble de la forêt, nous avons choisi le déploiement grâce à l'installation à distance. Nous soulignons que nous avons installé l'antivirus après l'installation du contrôleur de domaine pour profiter des avantages d'installation de Kaspersky dans un domaine.

Au lancement de Kaspersky un assistant de configuration initial, nous demande de spécifier les paramètres des notifications par courrier, alors nous saisissons les informations requises.

Figure III.22 : Spécification des paramètres des notifications par courrier.

L'étape suivante nous donne le choix de saisir la clé maintenant ou plus tard, et lancer ou pas le processus de déploiement. Après avoir confirmé le processus de déploiement, l'assistant d'installation à distance s'ouvre.

Figure III.23: Assistant d'installation à distance.

Sélectionnons le paquet d'installation parmi la liste donnée, ou créons un autre, puis déployons l'agent d'administration.

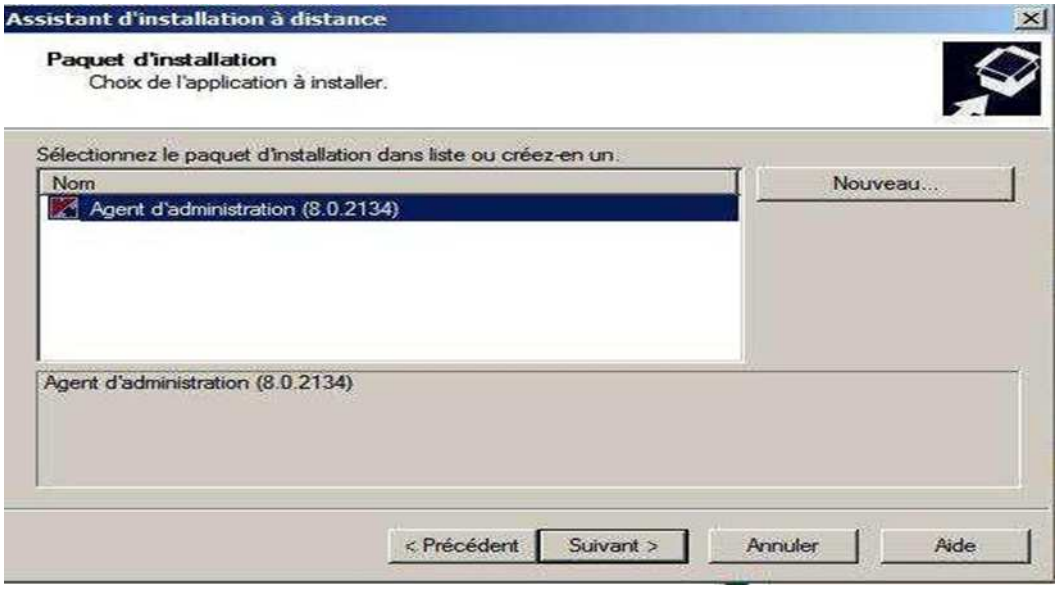


Figure III.24 : La sélection de paquet d'installation.

Maintenant, sélectionnons l'ensemble de la forêt**2intparteners.com** pour le déploiement de l'antivirus.

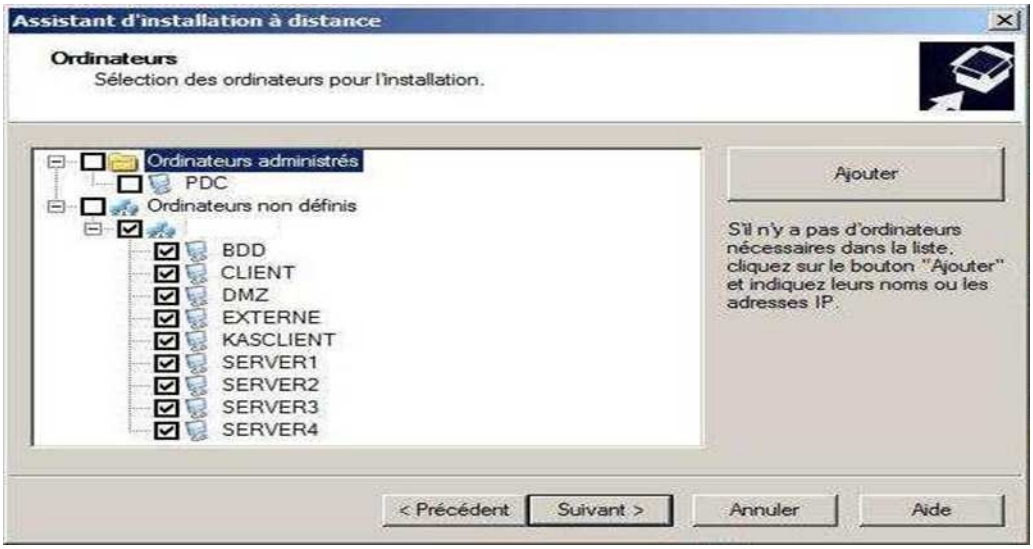


Figure III.25: La sélection des ordinateurs pour l'installation.

L'étape suivante consiste à définir les paramètres d'installation à distance.

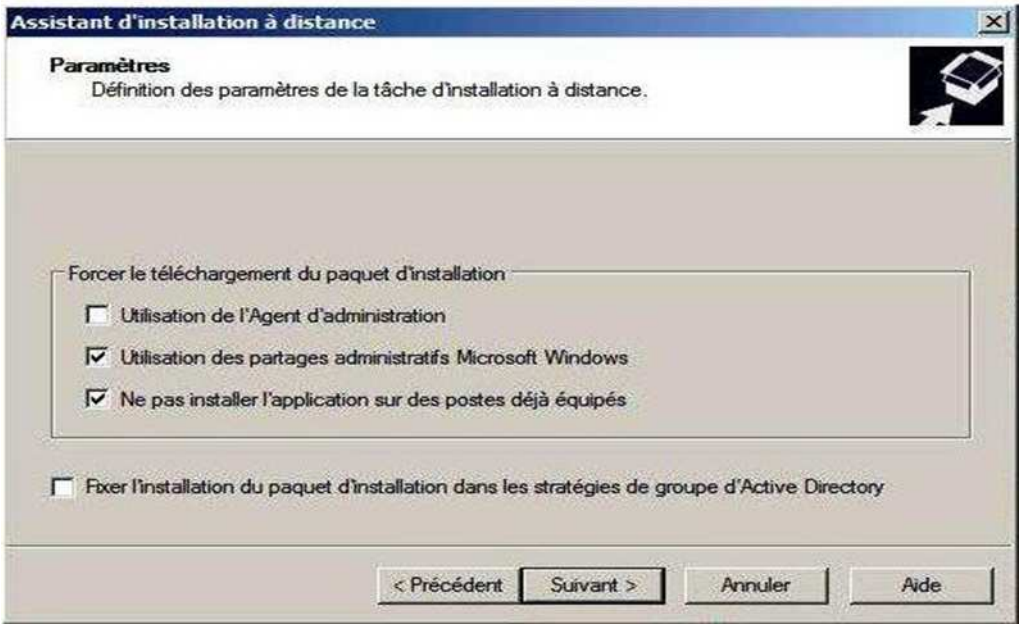


Figure III.26: La définition des paramètres d'installation à distance.

Définissons ci-après le compte avec lequel nous accédons aux ordinateurs de la forêt.

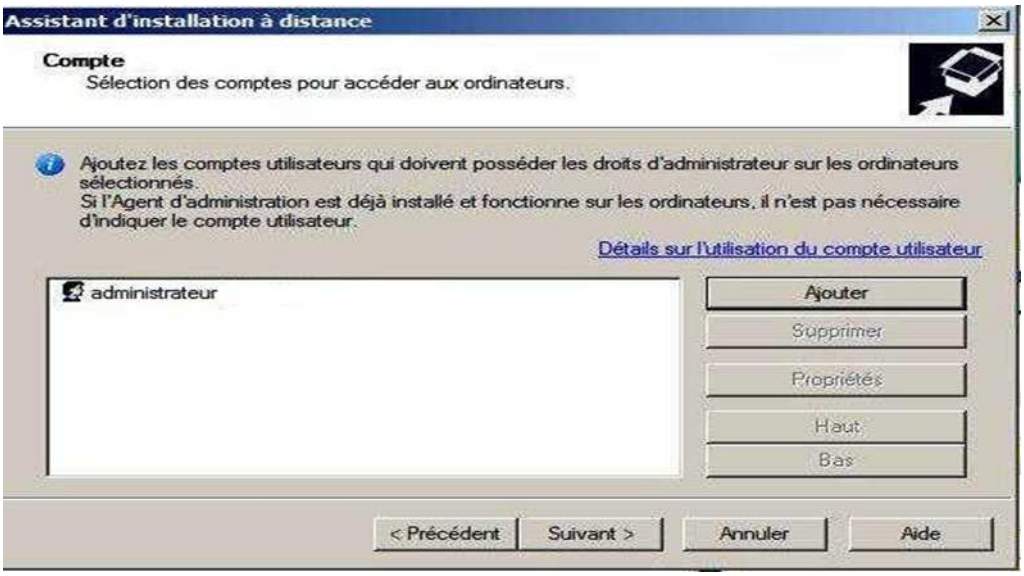


Figure III.27: Sélection du compte pour accéder aux ordinateurs.

Il nous reste plus qu'à lancer l'installation.

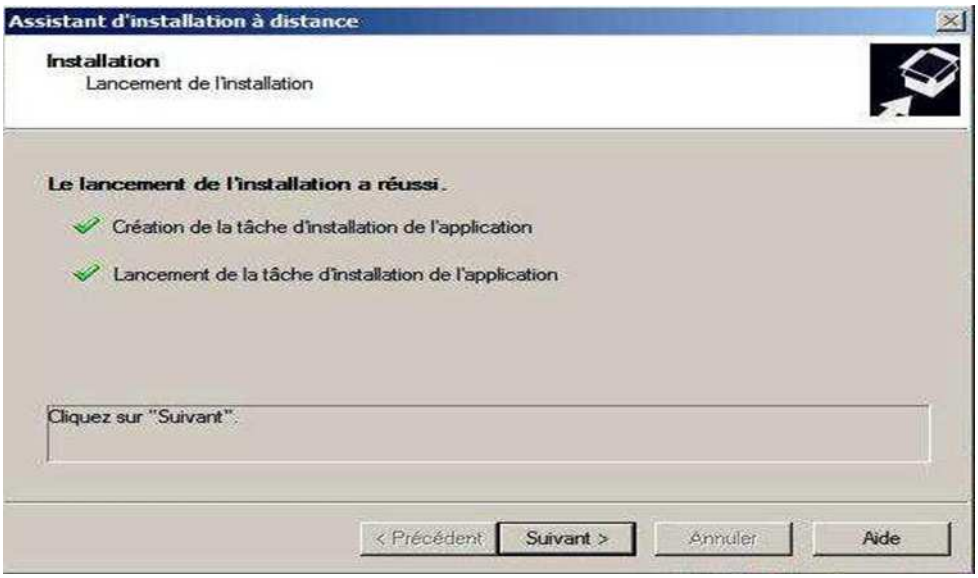


Figure III. 28.: Lancement de l'installation.

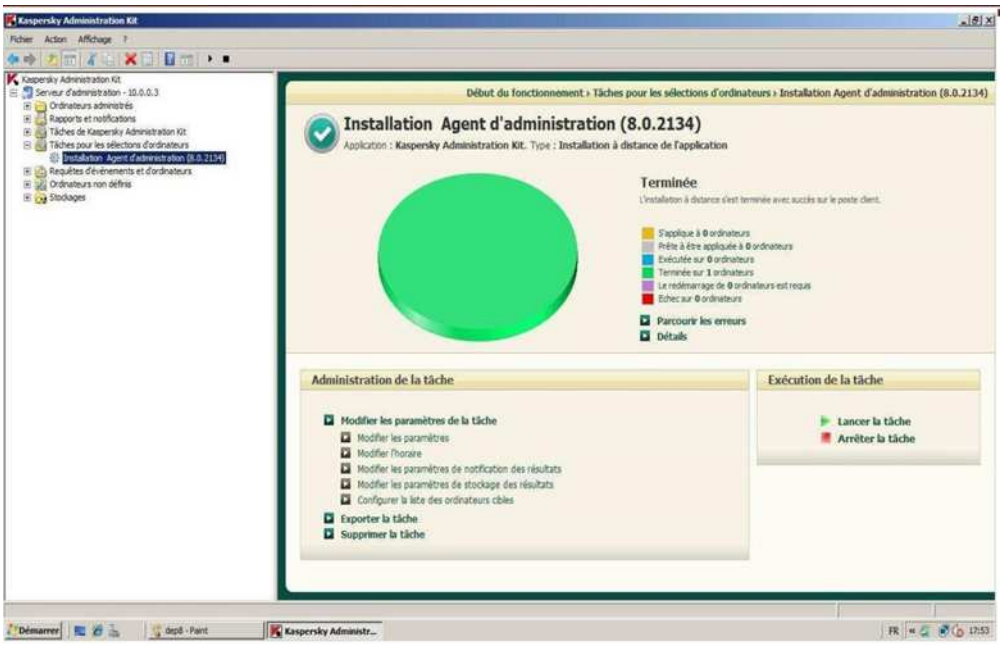


Figure III.29: Installation réussie.

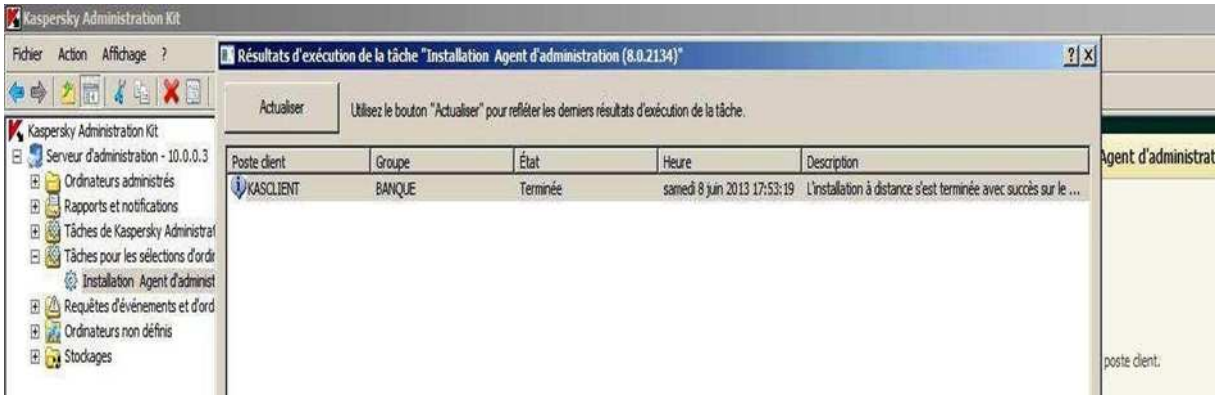


Figure III.30 : Installation réussie sur la machine client.

Si nous accédons aux programmes installés sur l'une des machines clients, nous trouvons Agent d'administration.

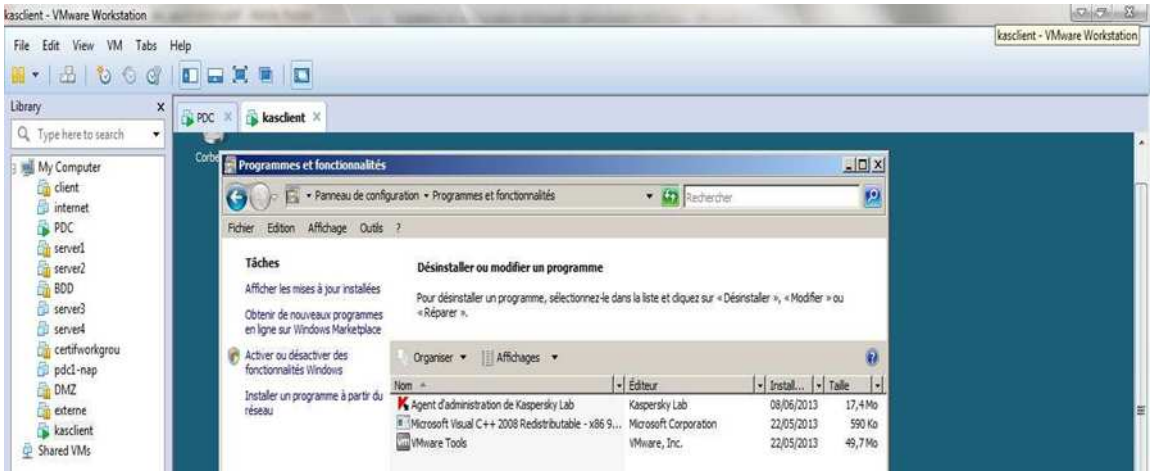


Figure III.31: Programmes installés sur la machine client.

III.2.4.Etape 4 : La connexion des machines sous GNS3

Apres avoir implémenté les différentes solutions concernant les machines virtuelles, nous les connectons à GNS3. Ensuite nous relions les différents serveurs et ordinateurs au firewall ASA, après avoir configuré ses interfaces.

a. La configuration de l'ASA sous GNS3

Dans cette section nous allons configurer l'ASA sous GNS3 afin de mieux expliquer cette procédure, nous accompagnons chaque étape d'une figure.

b. Le chargement de l'IOS de l'ASA

Pour que l'ASA fonctionne correctement il lui faut deux images IOS, l'une **.initrd** et l'autre**. Kernel** qui se charge en deux étapes dans l'ordre suivant:

La première étape consiste à charger l'image. **Initrd,** comme tout IOS.

La deuxième étape consiste à sélectionne l'ASA, dans le menu edit-> préférences->Qemu->ASA, en ajoutant l'image .initrd et .kernel, comme illustrée dans la figure ci-dessous, en spécifiant le nom la RAM et d'autre critères.

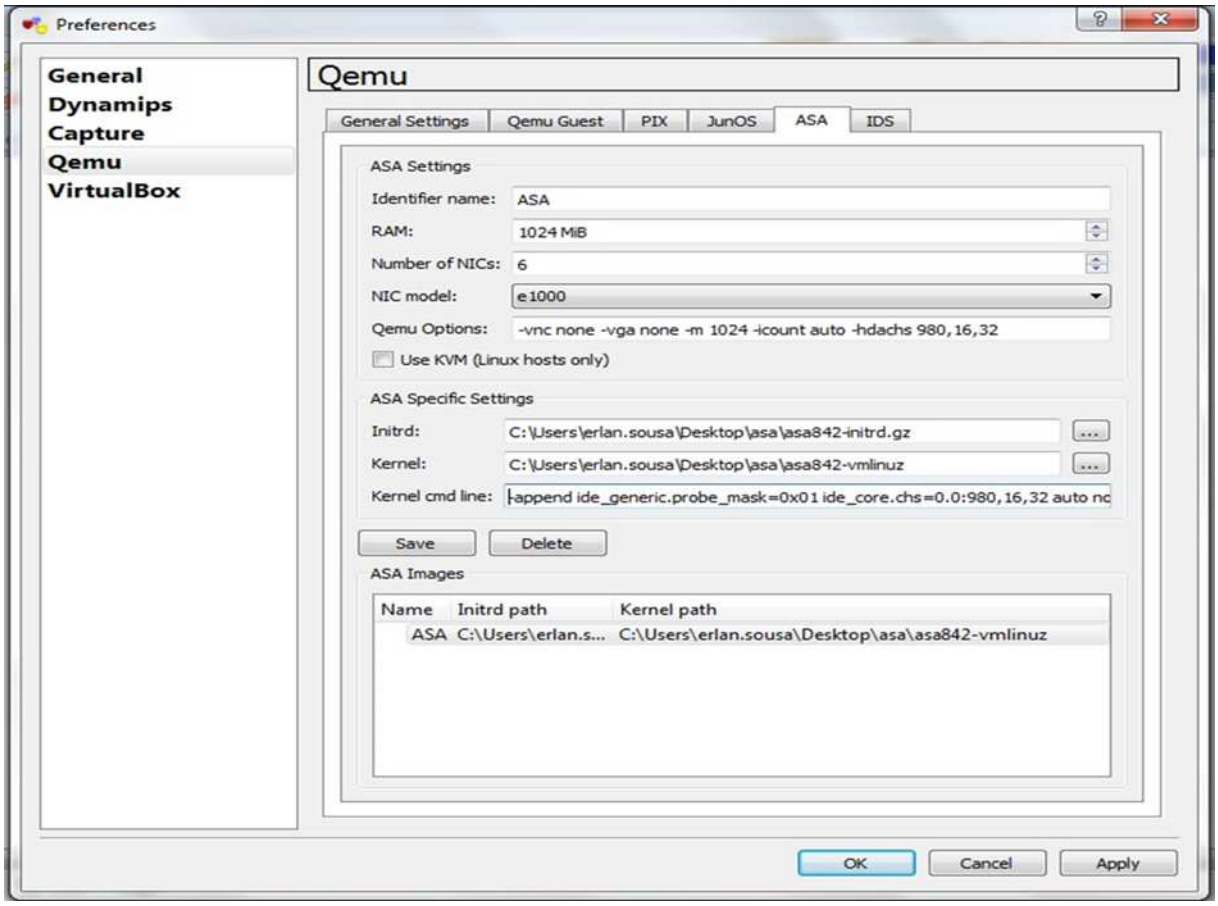


Figure III.32 :L'ajout de l'IOS pour l'ASA.

Maintenant que le chargement c'est fait, l'ASA est prêt à l'utilisation. Au démarrage de l'ASA une fenêtre s'ouvre QEMU**,** afin de pouvoir lancer la console de configuration, il faut garder cette dernière ouverte pendant toute la procédure de configuration.

Figure III.33: La fenêtre QEMU.

c. L'activation de la console

A l'ouverture de la console, un message d'activation de la console s'affiche, nous tapons les commandes suivantes comme la montre la figure ci-dessous pour activer la console.

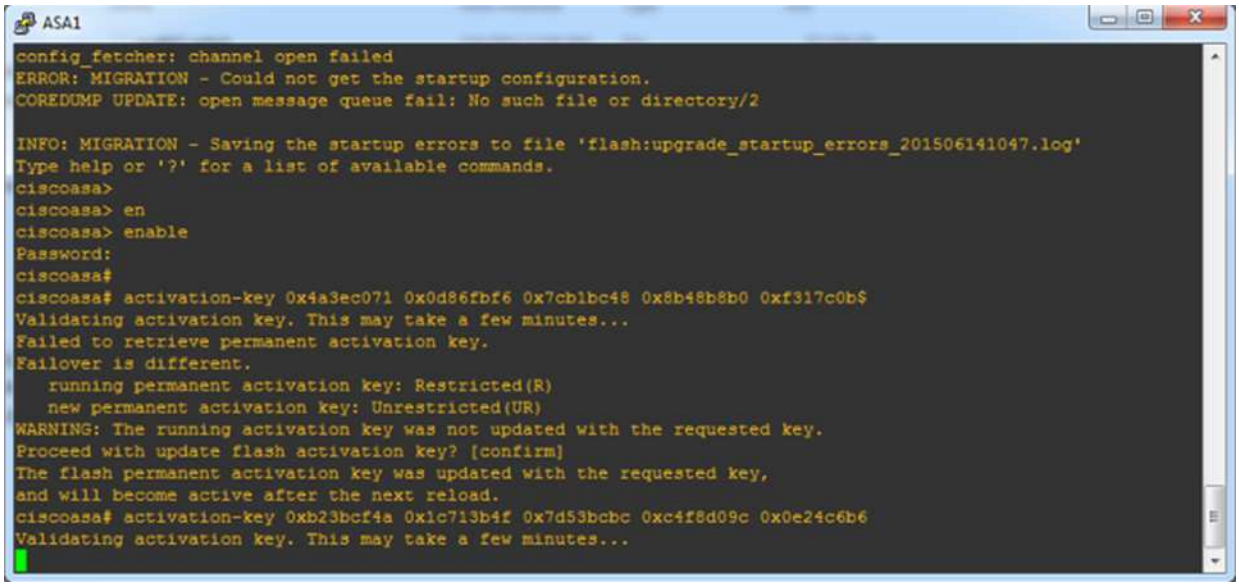


Figure III.34: Activation de la console.

d. La configuration des interfaces

L'attribution des adresses se fait comme tout autre équipement Cisco, néanmoins on doit préciser la nature de l'interface Inside ou outside et le niveau de sécurité de chaque interface.

Figure III.35 : La configuration des interfaces.

f. La création de l'identifiant de l'utilisateur

Afin de sécuriser l'accès lors de la configuration des règles de firewall ASA, il est nécessaire d'attribuer un identifiant, un mot de passe ainsi qu'un niveau de privilèges pour l'administrateur de firewall.

```
ciscoasa(config)# username 2int password cisco privilege 15
ciscoasa(config)# exit
ciscoasa# exit
```

Figure III.36: L'identification de l'utilisateur.

g. La configuration de l'http

Pour qu'une machine client puisse effectuer des requêtes HTTP, il faut le configurer au niveau de l'ASA.

```
ciscoasa(config)# asdm image flash:/asdm-711.bin
ciscoasa(config)# htt
ciscoasa(config)# http ser
ciscoasa(config)# http server en
ciscoasa(config)# http server enable
ciscoasa(config)# htt
ciscoasa(config)# http 10.0.0.128 255.255.255.255 inside
ciscoasa(config)# user
ciscoasa(config)# usern
ciscoasa(config)# username 2int ?
```

Figure III.37: La configuration de l'http.

h. Le chargement de l'ASDM

Pour pouvoir gérer et crée les règles de firewall ASA, il faut installer et lancer l'ASDM dans la machine distante (client).Pour cela suivons les étapes dans l'ordre que voici :

i. Installer ASDM dans le serveur TFTP

Copier le fichier TFTP et l'exécuter dans la machine client, puis ajouter l'image asdm-647.bin.

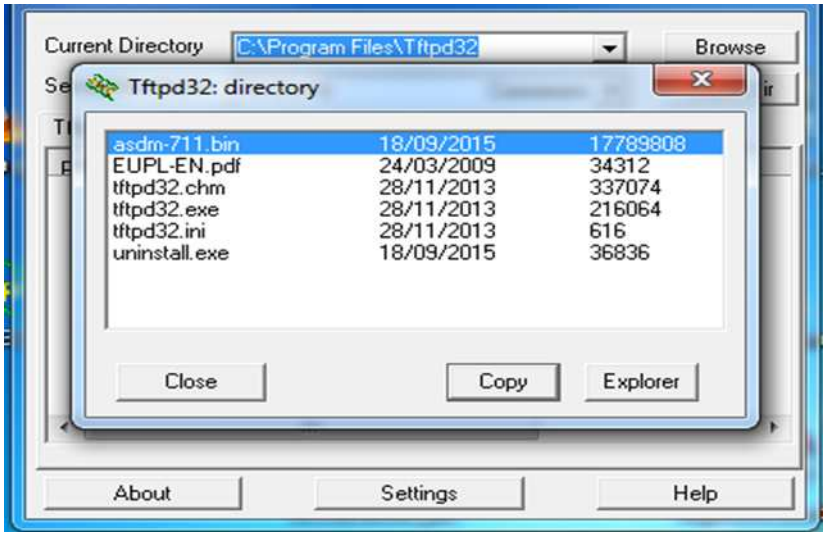


Figure III.38: Ajout de l'image ASDM à TFTP.

Maintenant, revenons à notre console ASA et chargeons l'image ASDM -647.bin en tapant les commandes suivantes :

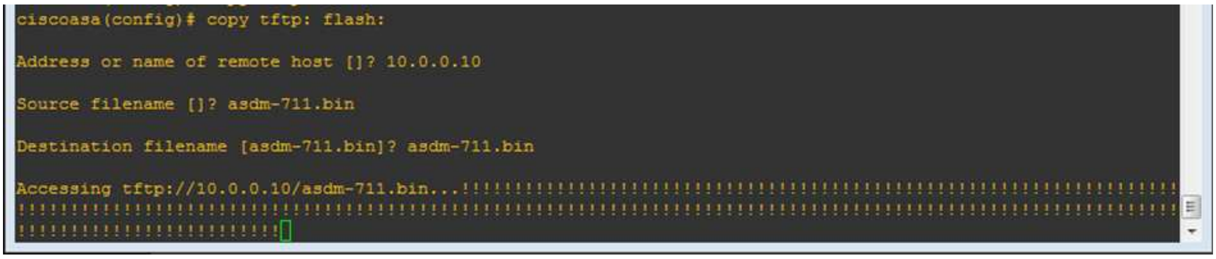


Figure III.39: Chargement de l'image ASDM.

j. La sauvegarde de la configuration

Après avoir fini notre configuration nous allons la sauvegarder.

Figure III.40: La sauvegarde de configuration.

k. Le lancement de l'ADSM

Avant le lancement d'ASDM, il faut s'assurer de la connexion entre l'interface de l'ASA et la machine distante en effectuant un **ping** dans les deux côtés.

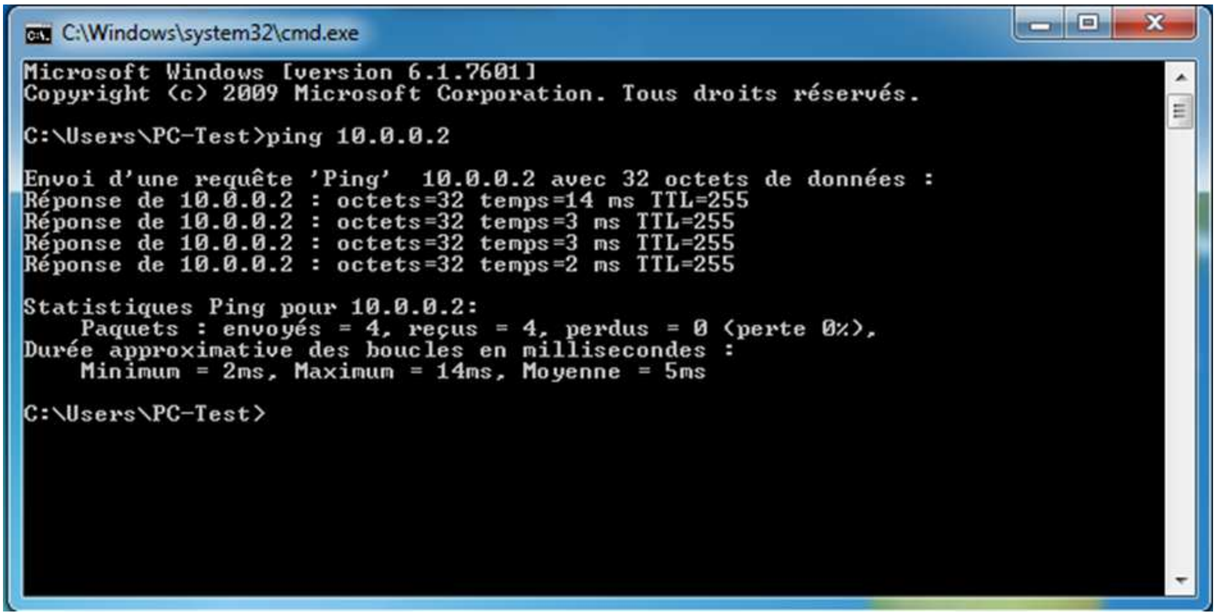


Figure III.41: Ping de la machine distante.

Figure III.42 : Ping de l'interface ASA.

A partir de l'internet explorer de la machine distante introduisons l'adresse https://10.0.0.2/ Dans la page qui s'ouvre cliquons sur poursuivre avec ce site web (non recommandé).

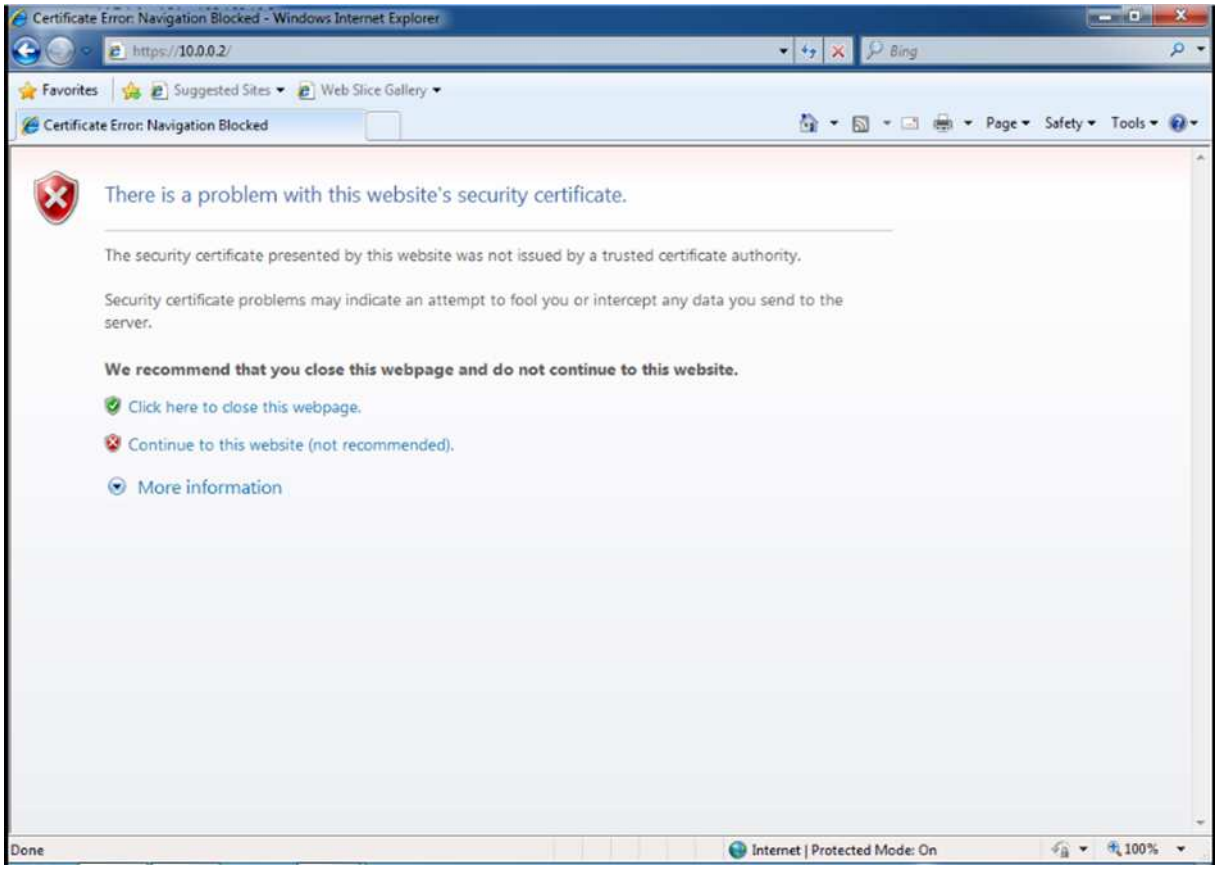


Figure III. 43.: Accès à l'interface d'ASA.

Cette page va nous ramener à l'interface de l'installation de l'ASDM.

Cliquons sur Install ASDM Launcher and Run ASDM.

Une fenêtre d'authentification s'ouvre, permettant à l'administrateur du firewall d'accéder, avec le nom d'utilisateur et mot de passe à l'interface graphique ASDM.

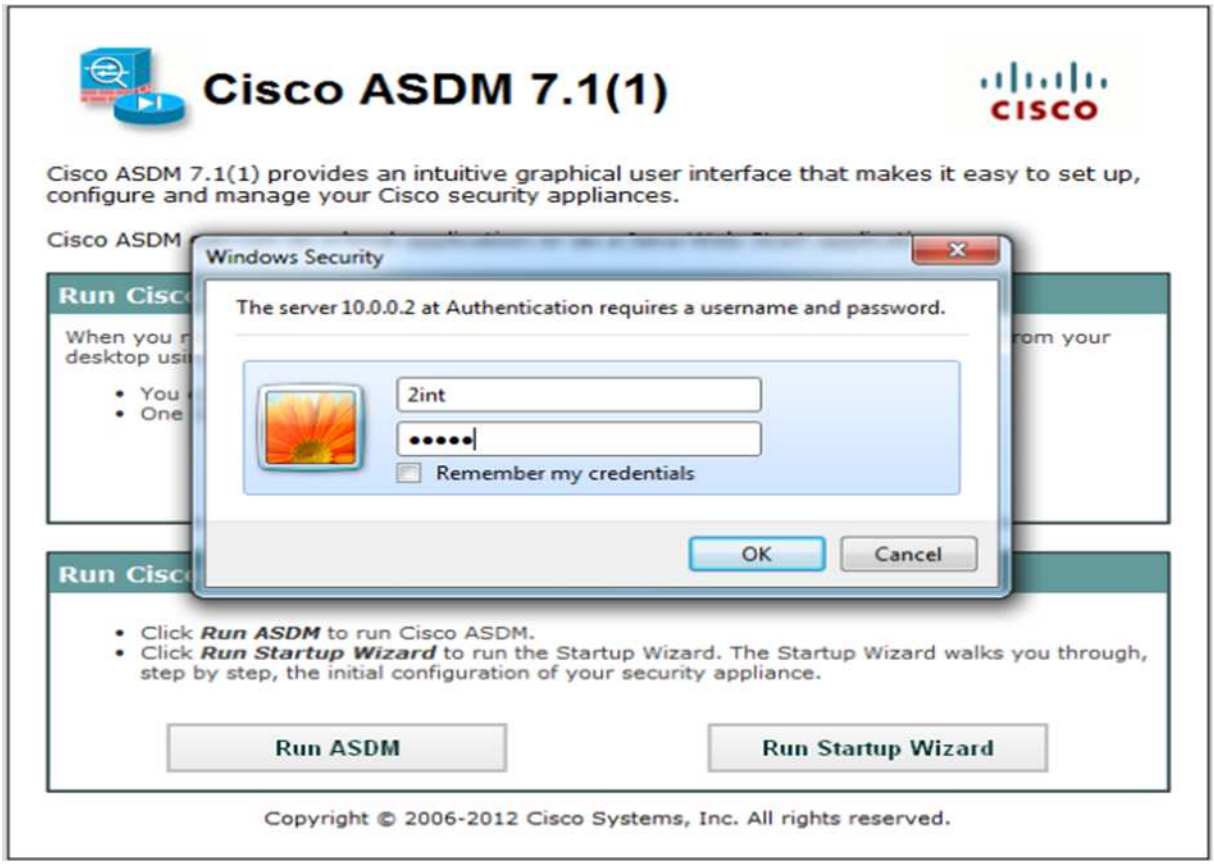


Figure III.44: L'authentification de l'utilisateur.

A la fin de l'installation, nous voyons l'interface ASDM dans le menu home.

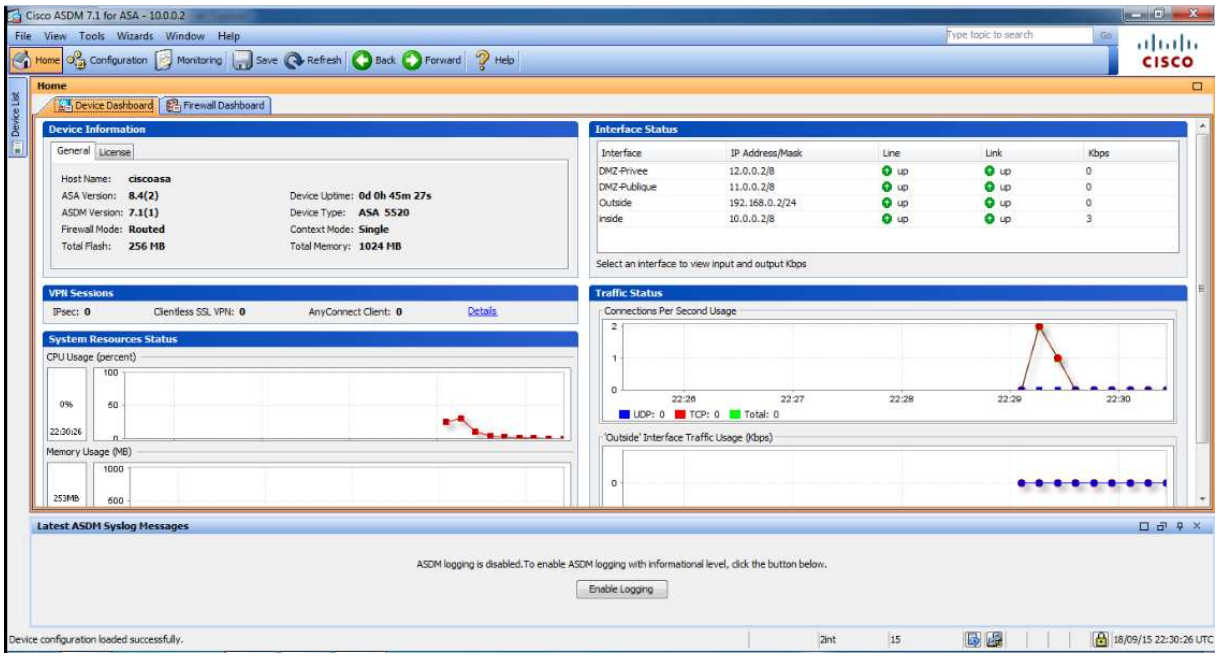


Figure III.45 : Le menu Home de l'interface ASDM.

Pour ajouter des règles à ce firewall nous accédons au menu configuration

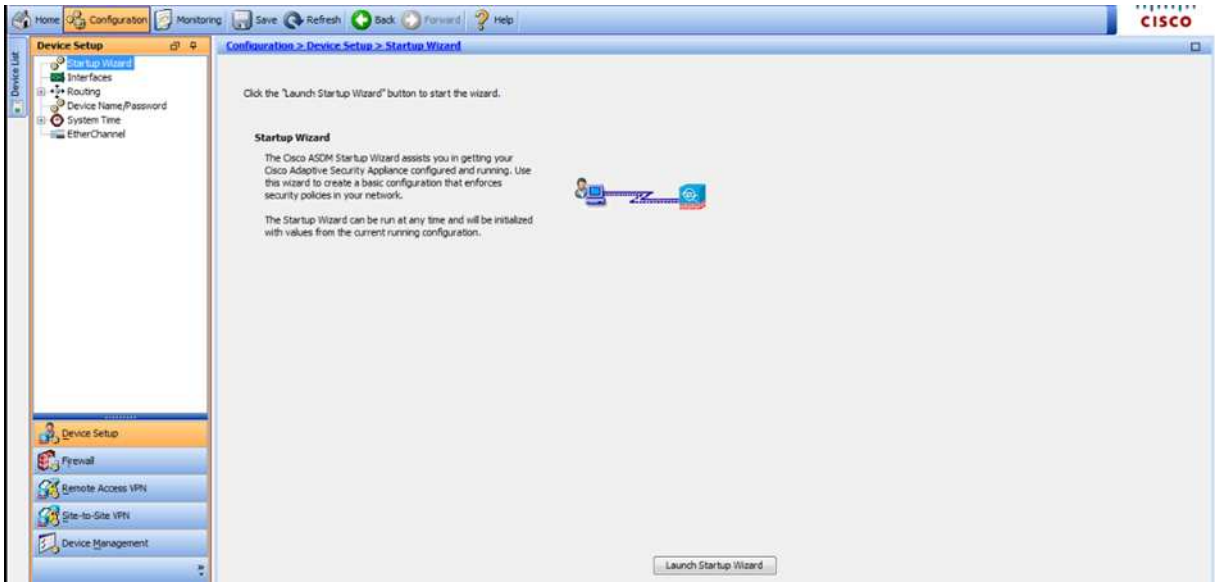


Figure III.46 : Menu configuration.

III.2.5.Création de la DMZ

Avant de créer la DMZ ASA, nous expliquons son principe de fonctionnement. Comme le montre l'architecture, l'ASA relie trois réseaux via trois interfaces.

ASA->Intranet (Intérieur) : L'interface **Inside** avec un niveau de sécurité 100.

ASA-> DMZ Publique (DHCP, Radius) : L'interface **DMZ** avec un niveau de sécurité 70.

ASA-> DMZ Privée (Web, Fichiers) : L'interface **DMZ** avec un niveau de sécurité 50.

ASA->internet (Extérieur) : L'interface **outside** avec un niveau de sécurité 0.

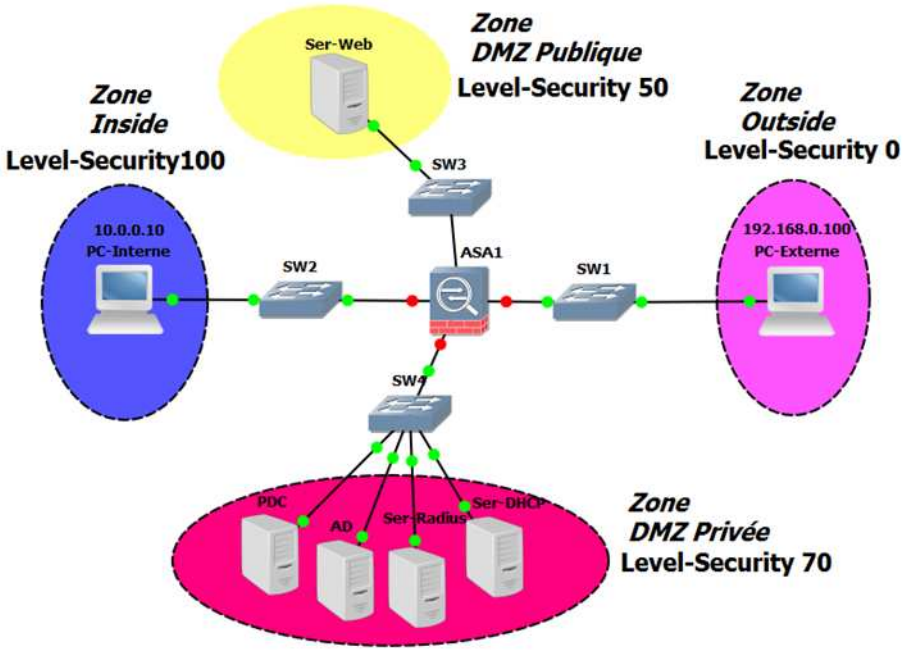


Figure III.47La DMZ ASA.

ASA->Intranet : L'interface Inside avec un niveau de sécurité 100.

ASA-> DMZ1 : L'interface DMZ avec un niveau de sécurité 70.

ASA-> DMZ1 : L'interface DMZ avec un niveau de sécurité 50.

ASA->internet : L'interface outside avec un niveau de sécurité 0.

Comme l'ASA ne permet pas le passage du trafic du niveau de sécurité supérieur à un niveau inférieur, dans cette architecture, le sens de trafic est comme suit :

De l'intranet->DMZ1 c'est permis (100->70).

De l'intranet->DMZ2 c'est permis (100->50).

De l'intranet->internet c'est permis (100->0).

De DMZ1->DMZ2 c'est permis (70->50).

De DMZ1->internet c'est permis (70->0).

De DMZ2->internet c'est permis (50->0).

De DMZ1->intranet n'est pas permis (70->100).

De DMZ2->DMZ1 n'est pas permis (50->70).

De l'internet->DMZ2 n'est pas permis (0->50).

De l'internet->DMZ1 n'est pas permis (0->70).

De l'internet->Intranet n'est pas permis (0->100).

De cette manière, nous assurons la protection l'entreprise de façon qu'aucun trafic ne puisse entrer.

Afin de configurer cette solution, nous accédons à l'interface graphique d'ASA, ASDM puis nous ajoutons les quatre interfaces Inside, outside, DMZ1 et DMZ2, en sélectionnant dans le menu configuration->interfaces->add interface**.**

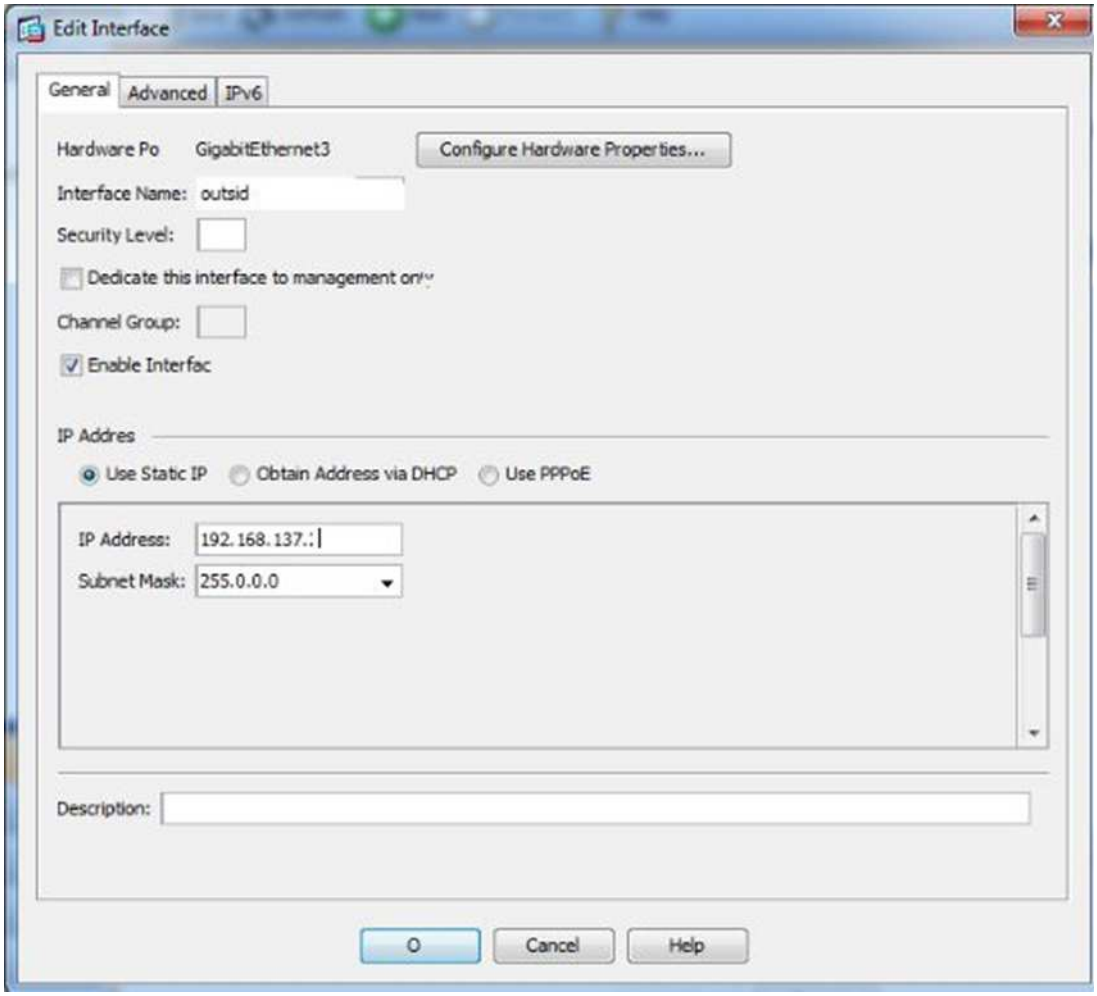


Figure III. 48 : Ajout d'une interface

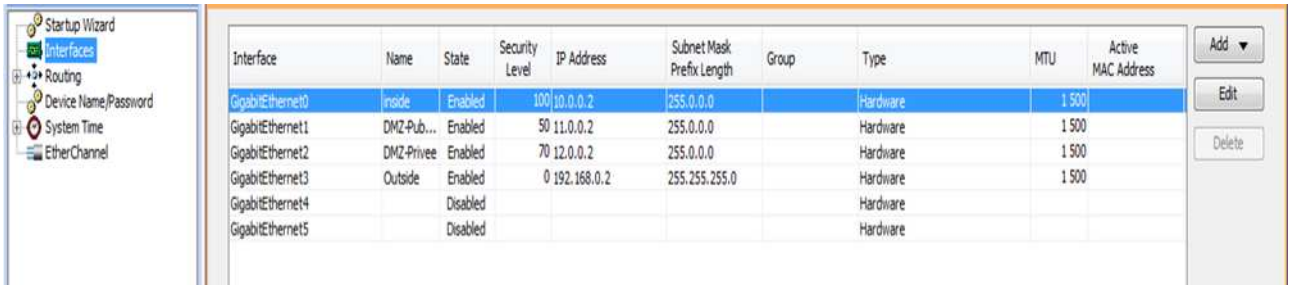


Figure III. 49 : L'ensemble des interfaces ajoutées.

III.2.6.Restriction du trafic

Comme nous l'avions dit, dans ASA par défaut, tout trafic de niveau supérieur à un niveau inférieur est permis, alors dans ce cas l'entreprise n'est pas protégée des malveillants internes qui peuvent faire sortir des informations critiques.

Pour cette raison nous avons restreint le trafic sortant et entrant, de manière n'autoriser que celui autorisé par l'entreprise. Pour ce que nous avons suggéré comme solution, et en se basant sur ce qui nous a été fourni comme informations sur les besoin de l'entreprise. Nous avons autorisé juste les protocoles de messagerie et web : Http, SMTP.

Et pour les autres protocoles concernant les applications et les échanges de l'entreprise avec ses partenaires, voire des informations confidentielles, nous n'avons pas pu les déterminer et nous avons laissé le soin à l'entreprise de les sélectionner.

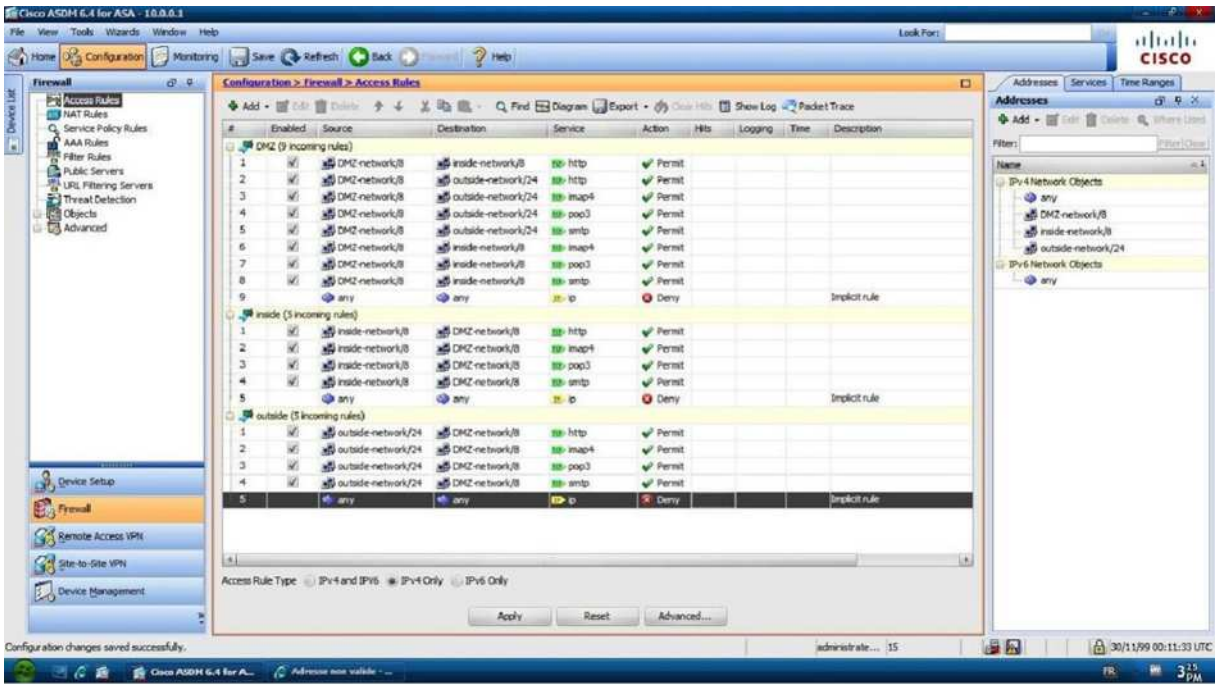


Figure III.50 : La restriction de trafic.

III.2.7.Configuration du NAT

Le réseau LAN dispose d'une plage d'adresse privée alors que la DMZ dispose d'une plage

Conclusion générale

La sécurité du système d'information d'une entreprise est un requis important pour la poursuite de ses activités .Qu'il s'agisse du vol de ses secrets de fabrication ou de la perte de ses données clients, et ça nous a ramené à parler de la nécessité de garantir certains besoins de sécurisation : l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que la non répudiation de ses actes.

Dans notre mémoire nous nous sommes intéressés à une technique (méthode) qui nous aide à mettre en place et en marche d'une infrastructure réseau sécurisée par la DMZ à l'aide de l'ASA Cisco 5510 , dans le but de faire face à ces différentes menaces et attaques, cette politique de sécurité qu'on a proposée est basée sur l'installation d'un firewall ainsi que la configuration des autres éléments d'interconnexions du réseau (routeur, fédérateur ,…….) afin d'avoir plus de sécurité en utilisant des listes de contrôle d'accès (ACL) et la translation d'adresses de l'entreprise.

En effet, la sécurité est comme une chaine et elle est proportionnelle aux différentes menaces qui augmentent au fur et à mesure c'est ce qui a fait de la sécurité un sujet très vaste et très important en même temps, donc nous envisageons quelques perspectives pour la continuation de ce travail :

- S'intéresser à d'autres aspects de sécurité comme par exemple : la configuration d'un VPN pour relier le réseau de l'entreprise 2int avec sa direction générale.
- Evaluation la solution en prenant en compte un autre aspect de sécurité tel que : L'authentification en utilisant le protocole RADIUS.
- Conception d'un réseau sans fil pour ajouter l'unité commerciale au réseau de l'entreprise.

Ce projet nous a permis d'enquérir des connaissances dans de nombreux domaines.

En effet il nous a initiés au monde de la recherche sur les réseaux surtout en ce qui concerne la sécurité. Il nous a également permis de découvrir le logiciel de simulation VMware Workstation, Windows server 2012, GNS3 d'annuaire Active directory ainsi que les protocoles qui les gèrent. Grace à notre modeste travail, nous avons eu l'occasion de voir beaucoup de choses de plus près et d'enrichir nos connaissances ; nous avons aussi eu la chance de mettre nos capacités en valeur et de faire face aux situations les plus critiques et obstacles et apprendre comment procéder pour s'en sortir.

Bibliographie

[1]J.F. Pillou « Tout sur la sécurité informatique », Ed. Dunod, 2005.

[2]J.F. Pillou « Tout sur les réseaux et internet », Ed.Dunod, 2007.

[3] [4] G.Pujolle, Eyrolles « initiation aux réseaux, », Ed. Dunod ; 2002.

[5] William .Puech « classification des réseaux » Centre Universitaire de Formation et de recherche, 2006.

[6]F.YADDADENE, N.TOUMI « Mise en œuvre d'une infrastructure réseau sécurisée par ISA server », mémoire de fin d'étude Master en électronique, UMMTO ,2012.

[7] S.ALICHE, A.HADDAD « Implémentation d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de TIZI OUZOU », mémoire de fin d'étude Master électronique, UMMTO, 2011.

[8] http:// WWW.idum.eu/spip.php? Article 237 Configuration de GNS3 pour la mise en place d'un pare –feu Cisco ASA

[9] Bernard. Cousin « Sécurité des réseaux informatique », Université de Rennes 1 ,2008.

[10] http:// WWW.google.fr/ le réseau informatique.

[11] http:// WWW.google.fr/ la sécurité des réseaux dans les entreprises.

[12] http :// WWW.google.fr/présentation Microsoft 2012 server.

[13] http: //WWW.Cisco.com/en

/US /products/swsecursw/ps2010/products_configuration_guide_book09186a00801172852.html:

[14] http:// WWW.google.fr/Cisco ASA server édition standard.